THÈSE

DE DOCTORAT DE TROISIÈME CYCLE DE MATHÉMATIQUES PURES

présentée

A L'UNIVERSITÉ SCIENTIFIQUE ET MÉDICALE
DE GRENOBLE

par

Juan TENA AYUSO

# RATIONALITE DES POINTS DE DIVISION PAR N D'UNE COURBE ELLIPTIQUE DEFINIE SUR $\mathbb{Q}$

Préparée dans le Laboratoire de Mathématiques Pures, associé au CNRS,

Soutenue le 28 juin 1973 devant la commission d'examen

Président : C. CHABAUTY Examinateurs : J.M. FONTAINE
J.R. JOLY

THÈSE

DE DOCTORAT DE TROISIÈME CYCLE DE MATHÉMATIQUES PURES

présentée

A L'UNIVERSITÉ SCIENTIFIQUE ET MÉDICALE
DE GRENOBLE

par

*Juan TENA AYUSO*

# RATIONALITE DES POINTS DE DIVISION PAR N D'UNE COURBE ELLIPTIQUE DEFINIE SUR $\mathbb{Q}$

Préparée dans le Laboratoire de Mathématiques Pures, associé au CNRS,
Soutenue le 28 juin 1973 devant la commission d'examen

Président: C. CHABAUTY Examinateurs: J.M. FONTAINE
J.R. JOLY

Digitized by the Internet Archive
in 2026

https://archive.org/details/IA41544319_0026

# SOMMAIRE


Pages

INTRODUCTION

CHAPITRE I - COURBES ELLIPTIQUES SUR UN CORPS PARFAIT I-1

§1 - Généralités et rappels ..... I-1
§2 - Corps de base $\mathbb{C}$ ..... I-4
§3 - Courbes elliptiques sur un corps fini ..... I-7
§4 - Courbes elliptiques sur un corps $\mathfrak{P}$-adique .... I-7
§5 - Courbes elliptiques sur un corps de nombres .. I-9

CHAPITRE II - ETUDE DES GROUPES DE CONGRUENCE $\Gamma_0(N)$ , $\Gamma_1(N)$ ET DES COURBES MODULAIRES ASSOCIEES II-1

§1 - Surfaces de Riemann associés à certains sous-groupes du groupe modulaire ..... II-1
§2 - Les groupes de congruences $\Gamma_0(N)$ et $\Gamma_1(N)$ .... II-2
§3 - Interprétation sur $\mathbb{C}$ en termes de courbes elliptiques ..... II-3
§4 - Interprétation sur $\mathbb{Q}$ en termes de courbes elliptiques ..... II-5

CHAPITRE III - ETUDE DES COURBES $Y_0(N)$ - APPLICATIONS III-1

§1 - Détermination effective des modèles $Y_0(N)$ ... III-1
§2 - Nullité du rang de $Y_0(N)$ ..... III-4
§3 - Calcul de $\rho_0(N)$ ..... III-9
§4 - Détermination de $\sigma_0(N)$ ..... III-11
§5 - Etude de $\mathcal{E}_0(N)_{\mathbb{Q}}$ . Conclusion ..... III-17
§6 - Applications ..... III-20

CHAPITRE IV - ETUDES DES COURBES $Y_1(N)$ . APPLICATIONS IV-1

§1 - Détermination effective de $Y_1(N)$ ..... IV-2
§2 - Etude de $Y_1(N)_{\mathbb{Q}}$ ..... IV-4
§3 - Conclusion ..... IV-5

BIBLIOGRAPHIE


-o-o-o-

# INTRODUCTION

Nous nous proposons, dans ce travail, de donner des résultats numériques sur l'ordre possible $N$ d'un point rationnel "exceptionnel" (c'est-à-dire d'ordre fini) d'une courbe elliptique sur $\mathbb{Q}$. Il existe à ce sujet deux conjectures :

(1) La "folklore conjecture" du rapport de Cassels [3] : "pour tout corps de nombres $k$ (et en particulier pour $\mathbb{Q}$), il existe une constante $C(k)$ ne dépendant que de $k$ et ayant la propriété suivante : si $E$ est une courbe elliptique sur $k$, et si $P$ est un point d'ordre $N$ de $E$, rationnel sur $k$, alors $N \leq C(k)$ ".

(Dem'janenko a publié récemment une "démonstration" de cette conjecture [4] : malheureusement, d'après Cassels [Math. Reviews, Sept. 1972], cette "démonstration" est incomplète ; elle ne donnerait de toute façon aucune indication sur la valeur de $C(k)$, même pour $k = \mathbb{Q}$).

(2) La "conjecture d'Ogg" ([16], p. 110) : "si $E$ est une courbe elliptique sur $\mathbb{Q}$, et si $P$ est un point d'ordre $N$ de $E$, rationnel sur $\mathbb{Q}$, on peut avoir $N = 1, 2, 3, \ldots, 10$ ou $12$, mais on ne peut pas avoir $N = 11$ ou $N \geq 13$ ". (En particulier, avec la notation de (1), on a $C(\mathbb{Q}) = 12$).

Comme nous nous limitons ici au corps de base $k = \mathbb{Q}$, seule la conjecture (2) nous intéresse en fait (pour l'interprétation de la liste des onze valeurs $1, 2, 3, \ldots, 10$ et $12$, voir [16], et le chap.IV) ; cette conjecture s'appuie notamment sur les résultats numériques suivants :

Valeurs possibles de $N$. - Dans [10], Lind donne des exemples de courbes elliptiques sur $\mathbb{Q}$ ayant un point rationnel d'ordre $2, 4, 6, 8, 10$ ou $12$. Dans [14], Nagell détermine les conditions auxquelles

doivent satisfaire les coefficients A et B d'une courbe elliptique $y^2 = x^3 - Ax - B$ pour qu'elle admette un point rationnel d'ordre N , et montre la possibilité d'une telle courbe (sur $\mathbb{Q}$) pour N = 3 , 4 , 5 , 6 , 7 , 9 .

Valeurs impossibles de N . - Dans [1] , Billing et Mahler prouvent l'impossibilité de N = 11 ; Lind [10] prouve celle de N = 16 , 20 ou 24 , Nagell [14] celle de N = 15 , Ogg [16] celle de N = 17 , puis [17] celle de N = 13 , 18 , et Swinnerton-Dyer (voir l'exposé [26]) celle de N = 37 . (L'exclusion des valeurs N = 13 , 18 , 37 est postérieure à la conjecture d'Ogg).

Dans ce travail, nous obtenons des résultats d'impossibilité analogues pour d'autres valeurs de N , et aussi (mais par d'autres méthodes) pour des valeurs signalées ci-dessus. Ainsi (chap. III, th. B et C) : impossibilité de N = 19 , 20 , 24 , 27 , 32 , 36 , 49 ; de même (chap. IV , th.A) : impossibilité de N = 11 , 14 , 15 .

Dans notre étude de ce problème des points rationnels d'ordre N , nous sommes amenés plus généralement à considérer l'existence de sous-groupes cycliques rationnels d'ordre N sur les courbes elliptiques sur $\mathbb{Q}$ . Le problème correspondant est la détermination des valeurs de N pour lesquelles il existe un couple (E,R) d'une courbe elliptique E sur $\mathbb{Q}$ et d'un sous-groupe cyclique R de E , d'ordre N et rationnel sur $\mathbb{Q}$ . On peut même, pour une valeur donnée de N , essayer de déterminer le nombre de classes (à $\mathbb{C}$-isomorphisme près) de tels couples (E,R) . Nous déterminons ici ce nombre (chap. III, th.A) pour les douze valeurs N = 11 , 14 , 15 , 17 , 19 , 20 , 21 , 24 , 27 , 32 , 36 , 49 . (Ce sont les valeurs de N pour lesquelles le genre de la surface de Riemann $X_o(N)$ associée au groupe de congruence $\Gamma_o(N)$ est égal à 1 ).

Le plan de ce travail est le suivant :

Dans le chapitre I, nous rappelons la théorie générale des courbes elliptiques sur un corps parfait $k$ (§1) , puis nous examinons en particulier les cas où $k$ est le corps $\mathbb{C}$ (§2) , un corps fini (§3) , un corps $\mathfrak{P}$-adique (§4) , ou un corps de nombres (§5) .

Dans le chapitre II, nous étudions brièvement le rapport existant entre l'ensemble $\mathcal{E}_o(N)$ (resp. $\mathcal{E}_1(N)$) des classes à $\mathbb{C}$-isomorphisme près de couples $(E,R)$ (resp. $(E,P)$) où $E$ est une courbe elliptique sur $\mathbb{C}$ et $R$ (resp. $P$) un sous-groupe cyclique (resp. un point) de $E$ d'ordre $N$ rationnel sur $\mathbb{C}$ , d'une part ; et la courbe $Y_o(N)$ (resp. $Y_1(N)$) , modèle projectif non singulier de la surface de Riemann $X_o(N)$ (resp. $X_1(N)$) associée naturellement au groupe de congruence $\Gamma_o(N)$ (resp. $\Gamma_1(N)$) , d'autre part. Nous obtenons ainsi le résultat suivant (prop.2) : pour $N \geq 4$ , il existe une correspondance bijective entre $\mathcal{E}_o(N)_{\mathbb{Q}}$ et l'ensemble des points de $Y_o(N)$ non paraboliques et rationnels sur $\mathbb{Q}$ . De même (prop.2) : pour $N \geq 7$ , il existe une correspondance bijective entre $\mathcal{E}_1(N)_{\mathbb{Q}}$ et l'ensemble des points de $Y_1(N)$ non paraboliques et rationnels sur $\mathbb{Q}$ .

Dans le chapitre III, nous appliquons les résultats du chapitre II à la détermination du cardinal $\varepsilon_o(N)$ de $\mathcal{E}_o(N)_{\mathbb{Q}}$ pour les douze valeurs $N = 11 , 14 , \ldots , 49$ pour lesquelles le genre de $Y_o(N)$ est égal à 1 . La liste des valeurs des $\varepsilon_o(N)$ est donnée p. 17 . On en déduit directement les résultats d'impossibilité annoncés pour $N = 20 , 24 , 32 , 36 , 49$ , et indirectement pour $N = 19 , 27$ . (Les équations des courbes $Y_o(N)$ sont déduites des "équations de Fricke").

Enfin, dans le chapitre IV , nous déterminons de même $\varepsilon_1(N)$ , cardinal de $\mathcal{E}_1(N)_{\mathbb{Q}}$ , pour les trois valeurs $N = 11 , 14 , 15$ pour lesquelles le genre de $Y_1(N)$ est égal à 1 , et nous constatons que $\varepsilon_1(N) = 0$ : d'où les résultats d'impossibilité annoncés pour $N = 11 , 14 , 15$ . (Les équations de $Y_1(11)$ , $Y_1(14)$ et $Y_1(15)$ sont obtenues par la "méthode de Billing et Mahler").

Monsieur J.R. JOLY m'a donné l'idée de ce travail et m'a prodigué son aide et ses conseils ; qu'il trouve ici l'expression de toute ma gratitude.

Monsieur C. CHABAUTY a bien voulu présider le jury et Monsieur J.M. FONTAINE en faire partie. Je les en remercie vivement.

Je tiens à remercier tout particulièrement Mme GUTTIN-LOMBARD et Messieurs GAUDE et GIRARD pour la compétence et la diligence avec lesquelles ils ont permis la réalisation matérielle de ce travail.

# CHAPITRE I

## COURBES ELLIPTIQUES SUR UN CORPS PARFAIT

### §1 - GENERALITES ET RAPPELS.

Soit $k$ un corps parfait.

Définition 1.1.

On appelle courbe elliptique sur $k$ toute courbe projective de genre 1, définie sur $k$ et ayant un point $O$ rationnel sur $k$.

Nous noterons $E$ une telle courbe et nous identifierons $E$ avec l'ensemble de ses points rationnels sur $\bar{k}$.

Proposition 1.1.

On peut munir $E$, d'une manière et d'une seule, d'une structure de variété abélienne, définie sur $k$, de dimension 1 et ayant $O$ pour élément neutre.

Voir [3], p. 211.

Nous noterons $(E,O)$, ou tout simplement $E$, la courbe elliptique munie d'une telle structure. Si l'ordre d'un point $P$ de $E$ est infini, $P$ est dit ordinaire ; autrement, $P$ est dit exceptionnel. L'ensemble des points exceptionnels de $E$ forme sa partie de torsion $E^t$, $E$ étant considéré comme $\mathbf{Z}$-module.

Proposition 1.2.

Si caract(k) $\neq 2,3$ , toute courbe elliptique sur k est birationnellement équivalente (isomorphe) à une courbe mise sous "forme normale de Weierstrass" :

$$y^2 = x^3 - Ax - B \ , \quad A,B \in k \ . \tag{1,1}$$

L'élément neutre de (1,1) est le point à l'infini.

Voir [3], théorème 7.1.

Proposition 1.3.

Soit E une courbe elliptique dans la forme (1,1). La somme de trois points de E est nulle (c'est-à-dire égale à l'élément neutre) si, et seulement si, ils sont alignés.

Voir [3], lemme 7.1.

Corollaire. Interprétation géométrique de la loi de groupe.

Soit E dans la forme (1,1) . Soient $P_1$ et $P_2$ deux points de E . Alors $P_{12} = P_1 + P_2$ est le symétrique, par rapport à l'axe Ox , du 3e point d'intersection avec E de la droite joignant $P_1$ et $P_2$ . Explicitement, on a les équations d'addition :

$$P_1(x_1,y_1) + P_2(x_2,y_2) = P_{12}(x_{12},y_{12})$$

$$x_{12} = \left(\frac{y_2-y_1}{x_2-x_1}\right)^2 - (x_1+x_2) \tag{1,2}$$

Si $P_1 = P_2$ , prenant la tangente en $P_1$ à E , on aura

$$x_{11} = \left(\frac{3x_1-A}{2y_1}\right)^2 - 2x_1 \tag{1,3}$$

Définition 1.2.

Soient $(E_1,O_1)$ $(E_2,O_2)$ deux courbes elliptiques définies sur $k$. On appelle isogénie (ou plus précisément $k$-isogénie) de $E_1$ sur $E_2$ toute application rationnelle $\lambda$ de $E_1$ sur $E_2$, définie sur $k$ et telle que $\lambda(O_1) = O_2$. On appelle degré de $\lambda$ le degré de l'extension algébrique $k(E_1)/k(E_2)$, $k(E_2)$ étant plongé dans $k(E_1)$ par l'intermédiaire de $\lambda$.

Proposition 1.4.

a) $\lambda$ est un homomorphisme pour les lois de groupe de $E_1$ et $E_2$.

b) la relation d'isogénie est symétrique : à $\lambda$ correspond une isogénie duale $\hat{\lambda}$ de $E_2$ sur $E_1$ telle que $\hat{\hat{\lambda}} = \lambda$ et degré $(\lambda)$=degré$(\hat{\lambda})$

c) $\ker(\lambda)$ est un sous-groupe fini de $E_1$ rationnel sur $k$. Si degré $(\lambda)$ est premier avec caract(k), alors card(ker $\lambda$) = degré $(\lambda)$.

Voir [3],§8.

En particulier, si $(E_1,O_1) = (E_2,O_2) = (E,O)$, une isogénie $\lambda$ est un endomorphisme de $(E,O)$. L'anneau $\mathrm{End}_k(E)$ est composé des isogénies de $E$ sur $E$ et de l'endomorphisme nul. Si $k$ est de caractéristique 0, $\mathrm{End}_k(E)$ entre dans l'un des deux cas suivants :

a) $\mathrm{End}_k(E) = \mathbb{Z}$.

b) $\mathrm{End}_k(E)$ est un ordre $\mathcal{O}$ d'un corps quadratique imaginaire.

Voir [3] p. 220. Dans le cas b) un élément $\lambda \in \mathrm{End}_k(E)$, $\lambda \notin \mathbb{Z}$ est appelé une multiplication complexe de $E$ (sur $k$).

Proposition 1.5.

Soit $E$ une courbe elliptique et soit $R$ un sous-groupe de $E$ rationnel sur $k$ et d'ordre fini. Il existe alors une courbe elliptique $E'$ (qu'on peut noter $E/R$) et une isogénie $\lambda$ (toutes deux définies sur $k$) : $E \to E'$, telles que $\ker(\lambda) = R$. Le couple $(E',\lambda)$ est unique à isomorphisme près.

Voir [3] lemme 8.5.

On appelle une telle isogénie, division de $E$ par le sous-groupe $R$. En particulier, soit $P$ un point d'ordre $N$ rationnel sur $k$ ; il engendre un groupe cyclique $R(P)$ d'ordre $N$ rationnel sur $k$ : l'isogénie $\lambda : E \to E/R(P)$ est parfois dite (improprement) division de $E$ par $N$. On étudiera un peu plus loin le cas où $N = 2$ (§2).

## §2 - CORPS DE BASE $\mathbb{C}$.

Soit $E$ une courbe elliptique sous la forme normale (1,1) avec les coefficients $A,B \in \mathbb{C}$. L'analyse classique montre que $E$ admet le paramétrage :

$$x = \wp(u) \quad , \quad y = 1/2\ \wp'(u) \qquad (1,4)$$

ou $\wp(u)$ est la fonction de Weierstrass correspondant au réseau $\Lambda$ d'invariants modulaires $g_2 = 4A$ , $g_3 = 4B$. $E$ s'identifie ainsi au tore complexe $\mathbb{C}/\Lambda$.

Soient

$$H = \{z \in \mathbb{C} \mid \mathrm{Im}(z) > 0\} \ ;$$

$$\Gamma = \mathrm{PSL}_2(\mathbb{Z}) \ , \text{ groupe modulaire ;}$$

$$D = \{z \in H \mid |z| > 1 \text{ et } |\mathrm{Re}(z)| < 1/2 \text{ , ou } |z| \geq 1 \text{ et } -1/2 \leq \mathrm{Re}(z) \leq 0\}$$

$D$ est un domaine fondamental pour $\Gamma$, c'est-à-dire un système complet de représentants pour $\Gamma$ agissant sur $H$.

Il est toujours possible de prendre une base $(\omega_1, \omega_2)$ de $\Lambda$ telle que $z = \omega_1/\omega_2 \in D$. La courbe $E$ est déterminée (à $\mathbb{C}$ isomorphisme près) par la valeur de l'invariant modulaire $j(E) = j(\omega_1/\omega_2)$. La fonction $j$ établit une application bijective et continue de $D$, donc de l'ensemble $\mathcal{E}$ des classes de courbes elliptiques sur $\mathbb{C}$, sur le corps $\mathbb{C}$.

Voir [20] Ch. IV.

A partir du paramétrage (1,4) et des propriétés de $\wp(u)$ on obtient ceci :

a) Soient $P_1$ , $P_2$ deux points de $E$ d'arguments elliptiques $u_1, u_2$ . Le point $P_{12}$ a pour argument $u_1+u_2$ . Trois points $P_1$ , $P_2$ , $P_3$ sont alignés si, et seulement si, les arguments elliptiques correspondants vérifient : $u_1 + u_2 + u_3 \equiv 0 \pmod{\Lambda}$ . En particulier les formules (1,2) et (1,3) sont la traduction de la formule d'addition bien connue de $\wp(u)$ .

b) $P$ est d'ordre $N$ si et seulement si $N$ est minimal pour la propriété : $Nu \equiv 0 \pmod{\Lambda}$ , $N > 0$ .

Application : division d'une courbe elliptique par un groupe cyclique d'ordre $N$ .

Soit $E$ une courbe elliptique sur $\mathbb{C}$ . Soit $R$ le sous-groupe cyclique engendré par un point $P$ d'ordre $N$ . On va appliquer la proposition 1.5 à la division de $E$ par $R$ . On fera usage des propriétés de la fonction $\wp(u)$ pour calculer explicitement $E' = E/R$ , mais on verra que le procédé est généralisable au cas d'un corps parfait quelconque.

Soit $\Lambda$ un réseau correspondant à $E$ et soient $g_2 = 4A$ , $g_3 = 4B$ ses invariants modulaires. On peut toujours choisir une base $(\omega_1, \omega_2)$ de $\Lambda$ et un point $P$ générateur de $R$ tels que $P$ ait $\omega_2/N$ comme argument elliptique.

Proposition 1.6.

*Le réseau $\Lambda'$ correspondant à $E'$ a pour base $(\omega_1, \omega_2/N)$ et $\lambda : E \to E'$ est induite par l'application*

$$z \pmod{\Lambda} \to z \pmod{\Lambda'} \qquad z \in \mathbb{C} \ .$$

Démonstration : Evidente. Faire le quotient de $E$ par le sous-groupe engendré par $P$ équivaut à faire le quotient de $\mathbb{C}/\Lambda$ par le sous-groupe cyclique engendré par $\omega_2/N$ .

Exercice : Calculons $E'$ explicitement pour $N = 2$ .

Soit $E$ dans la forme $(1,1)$ , et soit $P$ un point d'ordre 2 de $E$ . Il est du type $(\alpha,0)$ où $\alpha$ est une racine du polynôme $x^3-Ax-B$ . Par translation de l'origine au point $P$ , la courbe elliptique prend la forme

$$y^2 = x^3+Mx^2+Nx \qquad M,N \in \mathbb{C} \qquad (1,5)$$

avec les formules de transformation :

$$g_2 = 4A = 4(\frac{M^2}{3} - N)$$
$$g_3 = 4B = 4(\frac{MN}{3} - \frac{2M^3}{27}) . \qquad (1,6)$$

Proposition 1.7.

La courbe elliptique $E'$ a pour équation :

$$y'^2 = x'^3 - 2Mx'^2 + (M^2-4N)x' . \qquad (1,7)$$

Démonstration : D'après (1,6) il suffit de voir que les invariants $g'_2$ , $g'_3$ de $E'$ admettent l'expression :

$$g'_2 = 4(\frac{M^2}{3} + 4N)$$
$$g'_3 = 4(\frac{8MN}{3} - \frac{2M}{27}) .$$

Voyons-le pour $g'_2$

$$g'_2 = 60 \sum_{\omega\in\mathfrak{L}'}{}' 1/\omega^4 = 60 \sum_{\omega\in\mathfrak{L}}{}' 1/\omega^4 + 60 \sum_{\omega\in\mathfrak{L}} \frac{1}{(\omega_2/2+\omega)^4} = g_2 + 10\,\wp''(\omega_2/2)$$

$$= g_2 + 10(6\wp^2(\omega_2/2) - g_2/2) = -4g_2 + 60M^2/9 = 4(M^2/3+4N)$$

L'isogénie $\lambda$ de la courbe (1,5) sur la courbe (1,7) est donné par les équations

$$x' = y^2/x^2 \qquad y' = y(x^2-M)/x^2 \ . \qquad (1,8)$$

Remarque.

Les résultats ci-dessus sont applicables à un corps parfait arbitraire $k$ . Ainsi, si on suppose la courbe elliptique $E$ donnée par l'équation (1,5) , il suffit de prendre comme courbe quotient $E'$ la courbe donnée par l'équation (1,7), et de prendre comme $\lambda$ l'isogénie définie sur $k$ par les équations (1,8) .

## §3 - COURBES ELLIPTIQUES SUR UN CORPS FINI.

Soit $k$ un corps fini à $q$ éléments et de caractéristique $p$ . Toute courbe projective de genre 1 définie sur $k$ admet un point rationnel sur $k$ (Théorème de Schmidt) et donc est une courbe elliptique dans le sens de la définition 1.1. Voir [3] th. 15.1.

Soit $E$ une telle courbe elliptique définie sur $k$ . Il est évident que la partie rationnelle $E_k$ est finie , et donc que $E_k = E_k^t$ . Soit $N = \mathrm{Card}(E_k)$ . Une borne de $N$ est donnée en fonction de $q = \mathrm{Card}(k)$ par le théorème de Hasse:

$$|N-q-1| \leq 2q^{1/2} \qquad (1,9)$$

Voir [3], §15 . Pour une démonstration élémentaire (d'après Manin) voir [6], chapitre 10 , ou [22] .

## §4 - COURBES ELLIPTIQUES SUR UN CORPS $\mathfrak{P}$-ADIQUE.

Soit maintenant $k$ un corps $\mathfrak{P}$-adique, extension finie du corps $\mathbb{Q}_p$ . Soient $O_k$ l'anneau des entiers de $k$ , $\mathfrak{P}$ son idéal maximal,

$\tilde{k} = O_k/\mathfrak{P}$ le corps résiduel de $k$, et $|.|$ la valeur absolue associée à la valuation de $k$.

Soit $E$ une courbe elliptique dans la forme (1,1) définie sur $k$. Sans perdre en généralité, on peut supposer $A,B \in O_k$. L'interprétation analytique établie au §2 pour $k = \mathbb{C}$ n'a plus de sens. Pourtant on peut définir un "invariant" $j(E)$ (formellement) par la formule

$$j(E) = \frac{4.1728.A^3}{4A^3 - 27B^2} \qquad (1,10)$$

et on peut établir le résultat suivant :

Proposition 1.8.

*Soit $E$ une courbe elliptique définie sur $k$ et telle que*

i) $|j(E)| > 1$ b) $-1/2\ A/B \equiv 1 \pmod{k^{*2}}$ .

*Alors, il est encore possible de paramétrer $E$ par des fonctions $\wp$, $D_\wp$ construites à l'aide de fonctions théta, lesquelles coïncident formellement avec celles de l'analyse classique, si on considère, pour celles-ci, leur développement à l'infini.*

Voir [18] Ch.1 .

$\mathrm{Card}(E_k^t)$ est fini d'après le théorème de Nagell-Lutz (voir [11]). Pourtant la proposition suivante montre l'impossibilité d'établir un analogue au "théorème de Dem'janenko" pour les corps $\mathfrak{P}$-adiques.

Proposition 1.9.

*Quel que soit $N \geq 1$, il existe une courbe elliptique $E$ définie sur $k$ et admettant un point d'ordre $N$ rationnel sur $k$*

Voir [3] lemme 17.1. (Démonstration analytique, dans le style de la prop. 1.8).

Réduction modulo $\mathfrak{P}$ .

Soit $E$ une courbe elliptique sur $k$ dans la forme normale

$$E : y^2 = x^3 - Ax - B \quad .$$

La réduction de cette équation modulo $\mathfrak{P}$ nous donne une courbe $\tilde{E}$ définie sur $\tilde{k}$

$$\tilde{E} : y^2 = x^3 - \tilde{A}x - \tilde{B} \qquad \tilde{A},\tilde{B} \in \tilde{k} \quad .$$

Si $\tilde{E}$ est aussi une courbe elliptique, on dit que $E$ admet une bonne réduction modulo $\mathfrak{P}$ . L'application naturelle $\pi : E_k \to \tilde{E}_{\tilde{k}}$ est surjective. De plus :

Proposition 1.10.

$\pi$ est injective sur les points de $E_k^t$ d'ordre premier avec la caractéristique $p$ de $\tilde{k}$ . En particulier, si $\mathrm{Card}(E_k^t)$ est premier avec $p$ on a $\mathrm{Card}(E_k^t) = \mathrm{Card}(\tilde{E}_{\tilde{k}})$ .

Voir [3], § 19 .

## §5 - COURBES ELLIPTIQUES SUR UN CORPS DE NOMBRES.

Soit $k$ un corps de nombres et soit $E$ une courbe elliptique sur $k$ . En ce qui concerne la totalité des points de $E$ rationnels sur $k$ , on a le résultat suivant :

Proposition 1.11. (Théorème de Mordell-Weil)

$E_k$ est un groupe abélien (c'est-à-dire un $\mathbb{Z}$-module) de type fini. En d'autres termes, il existe dans $E_k$ $s$ points exceptionnels $P_1, P_2, \ldots, P_s$ et $r$ points ordinaires $P_{s+1}, \ldots, P_{s+r}$ (ces derniers linéairement indépendants sur $\mathbb{Z}$) tels que $E_k^t$ soit égal au sous-groupe de $E_k$ engendré par $P_1, \ldots, P_s$ et que $E_k$ lui-même soit engendré par $P_1, \ldots, P_s, P_{s+1}, \ldots, P_{s+r}$ .

Voir [12] , Ch.16. L'entier $r$ est le rang (sur $k$) de $E_k$ . Sa valeur peut en principe être déterminée par une méthode de "factorisation et descente" : voir [3], §24, et le chapitre III de ce travail.

En ce qui concerne seulement les points exceptionnels rationnels sur $k$ , on a d'autre part le résultat suivant de Lutz [11] et Nagell [13] :

Proposition 1.12.

*Supposons $k$ tel que $[k:\mathbb{Q}] \leq 3$ , et soit $P(x,y)$ un point exceptionnel de $E$ . Alors, $x$ et $y$ sont des entiers de $k$ , et (sauf si $y = 0$) $y^2$ divise le discriminant de $E$ .*

On fera usage de la proposition 1.12 dans le chapitre III, pour le cas $k = \mathbb{Q}$ , ainsi que de la remarque suivante :

Comme $\mathbb{Q} \subset \mathbb{Q}_p$ (ceci, quel que soit $p$ premier), on peut supposer $E$ définie sur $\mathbb{Q}_p$ . Si $E$ admet une bonne réduction modulo $p$ , la courbe réduite $\tilde{E}$ est une courbe elliptique dont les points rationnels sont facilement calculables. Par la proposition 1.11, on a une injection des points de $E^t_{\mathbb{Q}_p}$ d'ordre premier avec $p$ sur $\tilde{E}_{\mathbb{F}_p}$ dont une injection des points de $E^t_{\mathbb{Q}}$ d'ordre premier avec $p$ dans $\tilde{E}_{\mathbb{F}_p}$ . En particulier :

Proposition 1.13.

*Si $E$ , courbe elliptique définie sur $\mathbb{Q}$ , admet une bonne réduction modulo $p$ , et si l'ordre de $E^t_{\mathbb{Q}}$ est premier à $p$ , alors $\mathrm{Card}(E^t_{\mathbb{Q}})$ divise $\mathrm{Card}(\tilde{E}_{\mathbb{F}_p})$ .*

La réduction de $E$ modulo deux nombres premiers différents permet souvent de déterminer les points exceptionnels de $E$ sans avoir à appliquer la proposition 1.12.

Terminons ce paragraphe 5 en rappelant (voir l'introduction) les deux conjectures suivantes :

Conjecture 1.

L'ordre possible $N$ d'un point exceptionnel rationnel sur $k$ d'une courbe elliptique définie sur $k$ est borné par une constante ne dépendant que de $k$ .

Conjecture 2. (Ogg)

Pour $k = \mathbb{Q}$ , les seuls ordres possibles sont $N = 1,2,\ldots,10$ et 12, c'est-à-dire les onze valeurs de $N$ telles que le genre $p_1(N)$ de la surface de Riemann $X_1(N)$ soit égal à 0 . ($X_1(N)$ sera définie au chap. II,§2).

On vérifiera plus loin (Chap. III et IV) que les valeurs $N = 11,14,15,19\text{-}21,24,27,32,36,49$ , pour lesquelles le genre $p_o(N)$ de $X_o(N)$ égale 1 (voir chap.II) et pour lesquelles $p_1(N) \geq 1$ , sont "impossibles" (sur $k = \mathbb{Q}$) . Pour d'autres valeurs "impossibles" ($N = 11,13$, etc...), on renvoie à l'introduction.

# CHAPITRE II

## ETUDE DES GROUPES DE CONGRUENCE $\Gamma_o(N)$ , $\Gamma_1(N)$ ET DES COURBES MODULAIRES ASSOCIEES

Dans le chapitre I, §2, on a rappelé que $H/\Gamma$ établit un paramétrage de l'ensemble $\mathcal{E}$ des classes de courbes elliptiques sur $\mathbb{C}$. De façon plus précise, si on considère $\mathbb{P}_1(\mathbb{C})$ comme un modèle projectif de $H^*/\Gamma$ "via" l'invariant $j$, alors, pour tout corps $k$ tel que $\mathbb{Q} \subset k \subset \mathbb{C}$, on a une bijection entre $\mathcal{E}_k$ et $\mathbb{P}_1(k)-\{\infty\}$. Voir [20], p. 97.

Nous nous proposons maintenant de donner un paramétrage semblable pour les ensembles $\mathcal{E}_o(N)$ (resp. $\mathcal{E}_1(N)$) de couples $(E,R)$ (resp. $(E,P)$) formés d'une courbe elliptique $E$ et d'un sous-groupe cyclique, d'ordre fini $N$, de $E$ (resp. d'un point $P$ d'ordre $N$ de $E$), les couples étant définis à $\mathbb{C}$-isomorphisme près.

### §1 - SURFACES DE RIEMANN ASSOCIES A CERTAINS SOUS-GROUPES DU GROUPE MODULAIRE.

Soit $G \subset \Gamma$, d'indice fini $\mu = [\Gamma:G]$. Soient $\gamma_1,\ldots,\gamma_\mu$ des représentants des classes de $\Gamma$ modulo $G$. Un domaine fondamental pour

G est donné par :

$$D(G) = \bigcup_{i=1}^{\mu} \gamma_i D \quad .$$

$H^*/G$ est interprétable comme surface de Riemann compacte "au-dessus" de $\mathbb{P}_1(\mathbb{C})$, le revêtement $\pi : H^*/G \to \mathbb{P}_1(\mathbb{C})$ étant de degré $\mu$.

On appelle "diviseur parabolique" $\Delta$ de la surface de Riemann $H^*/G$ le diviseur $\pi^{-1}(\infty)$, c'est-à-dire l'image réciproque du point à l'infini de $\mathbb{P}_1(\mathbb{C})$ dans le revêtement. Soient $P_1,\ldots,P_\sigma$ les $\sigma$ points paraboliques non équivalents de G. On a alors, avec des conventions évidentes :

$$H^*/G = (H/G) \cup (P_1,\ldots,P_\sigma) \qquad \hat{D}(G) = D(G) \cup (P_1,\ldots P_\sigma) \quad .$$

Le genre $p(G)$ de la surface de Riemann $H^*/G$ est donné par la formule de Riemann-Hurwitz

$$2p(G) - 2 = -2\mu + \sum_{p \in H^*/G} (e_p - 1) \qquad (2,1)$$

Voir [20], p. 19.

## §2. LES GROUPES DE CONGRUENCES $\Gamma_0(N)$ ET $\Gamma_1(N)$ .

Définition 2.1.

On appelle groupe principal de congruence de niveau N le sous-groupe de $\Gamma$ défini par :

$$\Gamma(N) = \{\gamma \in \Gamma \ ; \ \gamma \equiv 1 \pmod N\} \quad .$$

Un sous-groupe G de $\Gamma$ est appelé groupe de congruence si, pour un certain N, $\Gamma(N) \subset G \subset \Gamma$. C'est le cas notamment pour les groupes $\Gamma_0(N)$ et $\Gamma_1(N)$ définis ci-dessous.

Définition 2.2.

On posera par la suite :

$$\Gamma_o(N) = \{\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma \; ; \; c \equiv 0 \pmod N\}$$

$$\Gamma_1(N) = \{\gamma \in \Gamma_o(N) \; ; \; a \equiv d \equiv 1 \pmod N\} \quad .$$

On notera $X_o(N) = H^*/\Gamma_o(N)$ , $X_1(N) = H^*/\Gamma_1(N)$ , les surfaces de Riemann correspondantes.

On aura alors, avec des notations évidentes, et pour une indexation convenable des points paraboliques :

$$\mu_o(N) = N \prod_{p/N} (1+p^{-1}) \qquad (= \psi(N) : \text{notation de Fricke}) \; ;$$

$$\mu_1(N) = N^2/2 \prod_{p/N} (1-p^{-2}) \; ; \qquad (2,2)$$

$$\Delta_o(N) = \sum_{d/N} d/t(P_{d,1}+\ldots+P_{d,\varphi(t)}) \; ;$$

$$\Delta_1(N) = \sum_{d/N} d(P_{d,1}+\ldots+P_{d,\varphi(N)/2.\varphi(t)/t}) \; ;$$

(t désignant le p.g.c.d. de d et N/d) .

Le genre $p_o(N)$ , $p_1(N)$ des surfaces de Riemann $X_o(N)$ , $X_1(N)$ est obtenu en adaptant la formule (2.1). Pour des expressions explicites voir [15], chap. IV, et [16].

## §3 - INTERPRETATION SUR $\mathbb{C}$ EN TERMES DE COURBES ELLIPTIQUES.

I. - Soient maintenant E une courbe elliptique définie sur $\mathbb{C}$ et R un sous-groupe cyclique d'ordre N de E . Notons (E,R) le couple formé de E et R , et soit ((E,R)) la classe de ce couple modulo la relation d'équivalence "$\sim$" ainsi définie : $(E,R) \sim (E',R')$ s'il existe un $\mathbb{C}$-isomorphisme $\lambda : E \xrightarrow{\sim} E'$ de courbes elliptiques tel

que $\lambda(R) = R'$ . Soit $\mathcal{E}_o(N)$ l'ensemble des classes $((E,R))$ , c'est-à-dire l'ensemble quotient de l'ensemble des couples $(E,R)$ par la relation d'équivalence "$\sim$" .

Proposition 2.1.

Il existe une bijection "naturelle" de $\mathcal{E}_o(N)$ sur $H/\Gamma_o(N)$ .

Démonstration : (indications) Soit $((E,R))$ un élément de $\mathcal{E}_o(N)$ et soit $\Lambda$ un réseau complexe associé à $E$ . En prenant une "bonne base" $(\omega_1,\omega_2)$ et un "bon" générateur de $R$ , on peut supposer $R$ engendré par le point d'argument elliptique $\omega_2/N$ .

Si alors un élément $\gamma = (a,b,c,d) \in \Gamma$ conserve le groupe $R$ , on doit avoir (pour un $m \in \mathbb{N}$) :

$$\gamma(\omega_2/N) \equiv m\omega_2/N \pmod{\Lambda} .$$

Comme $\gamma(\omega_2/N) = ((\omega_1+d\omega_2)/N$ , la condition ci-dessus équivaut à : $c \equiv 0 \pmod{N}$ , c'est-à-dire à $\gamma \in \Gamma_o(N)$ . Réciproquement, il est clair que tout élément de $\Gamma_o(N)$ conserve $R$ . D'où la proposition. On conviendra d'appeler la bijection inverse $H/\Gamma_o(N) \xrightarrow{\sim} \mathcal{E}_o(N)$ le "paramétrage naturel" de $\mathcal{E}_o(N)$ par $H/\Gamma_o(N)$ .

Remarque.

Le paramétrage de l'ensemble des sous-groupes cycliques d'ordre $N$ de $E$ par les classes de $\Gamma$ modulo $\Gamma_o(N)$ fournit une interprétation géométrique du degré $\mu_o(N) = \psi(N)$ du revêtement $X_o(N) \to X_o(1) = X(1)$ .

II. - Soit toujours $E$ une courbe elliptique définie sur $\mathbb{C}$ , et soit maintenant $P$ un point d'ordre $N$ de $E$ . Notons $(E,P)$ le couple formé de $E$ et $P$ , et soit $((E,P))$ la classe de ce couple modulo la relation d'équivalence "$\sim$" ainsi définie : $(E,P) \sim (E',P')$

s'il existe un $\mathbb{C}$-isomorphisme $\lambda : E \tilde{\to} E'$ tel que $\lambda(P) = P'$ .
Soit $\mathcal{E}_1(N)$ l'ensemble des classes $((E,P))$ , c'est-à-dire l'ensemble-quotient de l'ensemble des couples $(E,P)$ par la relation d'équivalence "$\sim$" .

Proposition 2.2.

*Il existe une bijection "naturelle" de $\mathcal{E}_1(N)$ sur $H/\Gamma_1(N)$ .*

Démonstration (indications) : Soit $((E,P))$ un élément de $\mathcal{E}_1(N)$ , et soit $\Lambda$ un réseau complexe associé à $E$ . On peut toujours supposer $P$ donné par un argument elliptique de la forme $m\omega_2/N$ (avec $(m,N) = 1$) par rapport à une "bonne base" $(\omega_1,\omega_2)$ de $\Lambda$ . Si alors un élément $\gamma = (a,b,c,d) \in \Gamma$ conserve le point $P$ , on doit avoir

$$\gamma(m\omega_2/N) \equiv m\omega_2/N \pmod{\Lambda} .$$

Comme $\gamma(\omega_2/N) = (c\omega_1+d\omega_2)/N$ , la condition ci-dessus implique $c \equiv 0$ , $d \equiv 1 \pmod N$ : d'où $\gamma \in \Gamma_1(N)$ . Réciproquement, il est clair que tout élément de $\Gamma_1(N)$ conserve $P$ . D'où la proposition. On conviendra d'appeler la bijection inverse $H/\Gamma_1(N) \tilde{\to} \mathcal{E}_1(N)$ le "paramétrage naturel" de $\mathcal{E}_1(N)$ par $H/\Gamma_1(N)$ .

Remarque.

Le degré du revêtement $X_1(N) \to X_o(N)$ est $\varphi(N)/2$ . Interprétation géométrique : un sous-groupe cyclique $R$ d'ordre $N$ admet $\varphi(N)$ générateurs $P$ , et d'autre part $(E,P) \sim (E,-P)$ . Donc, au-dessus d'un point de $X_o(N)$ , on doit trouver "en général" $\varphi(N)/2$ points de $X_1(N)$ .

## §4 - INTERPRETATION SUR $\mathbb{Q}$ EN TERMES DE COURBES ELLIPTIQUES.

Pour tout groupe de congruence $G$ , la surface de Riemann $H^*/G$ admet un modèle défini sur $\mathbb{Q}$ ; plus précisément, il existe un couple $(Y,\varphi)$ , où $Y$ est une courbe projective non-singulière définie sur $\mathbb{Q}$

et $\varphi$ une correspondance holomorphe et G-invariante de $H^*$ sur $Y$ qui établit une bijection de $H^*/G$ sur $Y$ .

Voir [20], Chap. 6, §7 .

Dans le cas particulier où $G = \Gamma_o(N)$ (resp. $\Gamma_1(N)$) nous noterons $Y_o(N)$ (resp. $Y_1(N)$) un tel modèle projectif non singulier.

I.- Introduction de $Y_o(N)$ .

Lemme 2.1.

$X_o(N)$ est la surface de Riemann de $v = j(N\tau)$ en tant que fonction algébrique de $u = j(\tau)$ .

Démonstration : Soit $u = j(\tau_1) = j(\tau_2)$ , ce qui implique $\tau_2 = \gamma\tau_1$ , $\gamma = (a,b,c,d) \in \Gamma$ . Voyons à quelle condition on a $j(N\tau_1) = j(N\tau_2)$ . Il faut (et suffit) pour cela que $N\tau_2 = \gamma' N\tau_1$ pour un $\gamma' = (a'b',c'd') \in \Gamma$ , donc que $\tau_2 = N^{-1}\gamma' N\tau_1 = (a'N^{-1}b', Nc'd')\tau_1 = \gamma\tau_1$ , donc en définitive que $c = \pm Nc'$ , c'est-à-dire $c \equiv 0 \pmod N$ , ou encore $\gamma \in \Gamma_o(N)$ . D'où le lemme, puisque $X_o(N) = H/\Gamma_o(N)$ .

Il résulte de là qu'un modèle affine de $X_o(N)$ est donné par la courbe $J_N$ d'équation $F_N(u,v) = 0$ (équation minimale reliant $u$ et $v$) dont le degré en $v$ (et en $u$ ) est $\mu_o(N) = \psi(N)$ = le degré du revêtement $X_o(N) \to X_o(1) = H/\Gamma$ . Cette équation peut s'écrire (voir par exemple [5]) :

$$F_N(u,v) = \prod_{\substack{a,b,d\geq 0 \\ ad=N \\ 0\leq b<d}} (v - j(\tfrac{a\tau+b}{d})) = 0 \qquad (2.3)$$

et on constate que $F_N(u,v)$ est un polynôme en $u$ et $v$ à coefficients dans $Z$ . Un modèle projectif non singulier $Y_o(N)$ peut alors (en principe) être obtenu à partir de $J_N$ par plongement projectif et désingularisation (en fait, on procède différemment : voir un peu plus bas "Modèles de Fricke", ainsi que le début du chap. III ; mais le modèle $J_N$ , "lieu du point $(j(\tau), j(N\tau)) = (u,v)$" , nous sera utile dans la démonstration du

théorème A ci-dessous).

Pour la démonstration du théorème A , nous aurons également besoin du lemme suivant :

Lemme 2.2.

Soit $\tau = \rho = e^{2i\pi/3}$ (resp. $\tau = i = \sqrt{-1}$) et soient a,b,d satisfaisant aux conditions de (2.3) . Alors, $j(\frac{a\tau+b}{d})$ n'est pas rationnel sur $\mathbb{Q}$ pour $N \geq$ (resp. $N \geq$ ) .

Démonstration : Soient $K = \mathbb{Q}(\tau)$ , A l'anneau des entiers de K , $\Lambda$ le réseau de base $(a\tau+b,d)$ , et $\mathcal{O}$ l'anneau des endomorphismes de $\Lambda$ : c'est un ordre de A , dont nous noterons f le conducteur. Il suffit de prouver que l'extension $K(j(\frac{a\tau+b}{d}))/K$ n'est pas triviale. Mais, par la théorie de la multiplication complexe, le degré de cette extension est égal au nombre $h_f$ de classes de $\mathcal{O}$ (voir [20], p. 106) lequel résulte de la formule

$$h_f = f.h_K.(A^*:\mathcal{O}^*)^{-1} \prod_{p|f} (1-(\tfrac{K}{p})p^{-1}) \quad .$$

Il suffit alors de vérifier que $h_f > 1$ pour $\tau = \rho$ et $N \geq 4$ (resp. 3) pour $\tau = i$ et $N \geq 3$) .

Venons-en au résultat essentiel de ce chapitre :

Théorème A.

Pour $N \geq 4$ , toute classe de $\mathcal{E}_o(N)$ "rationnelle sur $\mathbb{Q}$" (c'est-à-dire invariante par l'action "galoisienne" naturelle de $\mathrm{Aut}(\mathbb{C})$) est la classe d'un couple (E,R) où E est définie sur $\mathbb{Q}$ et où R est rationnel sur $\mathbb{Q}$ . En d'autres termes, le paramétrage naturel de $\mathcal{E}_o(N)$ par $J_N$ (voir prop. 2.1 et lemme 2.1) établit des bijections entre les trois ensembles suivants :

- l'ensemble $(J_N)_{\mathbb{Q}}$ ;

- l'ensemble $\mathcal{E}_o(N)_{\mathbb{Q}}$ ;

- l'ensemble des classes (à $\mathbb{C}$-isomorphisme près) de couples $(E,R)$ avec $E$ et $R$ rationnels sur $\mathbb{Q}$ .

Démonstration : i) Soit $((E,R)) \in \mathcal{E}_o(N)_{\mathbb{Q}}$ , et soit $\Lambda$ le réseau associé à $E$ . Prenons une base $(\omega_1,\omega_2)$ de $\Lambda$ telle que $R$ soit engendré par le point d'argument elliptique $\omega_2/N$ . Considérons la courbe $E' = E/R$ définie également sur $\mathbb{Q}$ (proposition 1.5) et dont le réseau associé est $\Lambda' = (\omega_1,\omega_2/N)$ .

Les invariants modulaires

$$j_E = j(\omega_1/\omega_2) = j(\tau) \quad , \quad j_{E'} = j(N\omega_1/\omega_2) = j(N\tau)$$

sont rationnels et $(j(\tau),j(N\tau))$ est donc un point rationnel de $J_N$ , c'est-à-dire un élément de $(J_N)_{\mathbb{Q}}$ .

ii) Inversement, soit $(u,v)$ un point rationnel de $J_N$ . Il existe un $\tau \in H$ tel que $u = j(\tau)$ , $v = j(N\tau)$ . Soient $E$ , $E'$ les courbes elliptiques associées aux réseaux $\Lambda$ , $\Lambda'$ de bases $(\tau,1)$ et $(\tau,1/N)$ :

$$j_E = j(\Lambda) = j(\tau) = u \quad , \quad j_{E'} = j(\Lambda') = j(N\tau) = v \quad .$$

Soit $\lambda : E \to E'$ l'isogénie de degré $N$ correspondant à la division de $E$ par le sous-groupe cyclique $R$ d'ordre $N$ engendré par $1/N$ . Alors $((E,R)) \in \mathcal{E}_o(N)$ , et correspond au point $(u,v)$ de $J_N$ . Comme la bijection $\mathcal{E}_o(N) \xrightarrow{\sim} J_N$ composée de $\mathcal{E}_o(N) \xrightarrow{\sim} H/\Gamma_o(N)$ et de $H/\Gamma_o(N) \xrightarrow{\sim} J_N$ commute évidemment à l'action "galoisienne" de $\mathrm{Aut}(\mathbb{C})$ , la rationalité de $(u,v)$ sur $\mathbb{Q}$ équivaut à l'assertion " $((E,R)) = ((E^\sigma,R^\sigma))$ pour tout $\sigma \in \mathrm{Aut}(\mathbb{C})$ " . D'autre part, $u = j_E \in \mathbb{Q}$ , et $E$ est définie sur $\mathbb{Q}$ , donc $E^\sigma = E$ . Ainsi, la rationalité de $(u,v)$ sur $\mathbb{Q}$ équivaut en fait à l'assertion "il existe un automorphisme $\lambda$ de $E$ tel que $\lambda(R) = R^\sigma$ " . Si alors $u \neq 0$ , $12^3 = 1728$ , $\mathrm{Aut}(E) = \{\pm 1\}$ , donc

$\lambda = \pm 1$ , et " $\lambda(R) = R^{\sigma}$ " s'écrit " $R = R^{\sigma}$ " . Ceci ayant lieu pour tout $\sigma \in \mathrm{Aut}(\mathbb{C})$ , $R$ est rationnel sur $\mathbb{Q}$ , ce qui prouve ii) dans le cas général (et sans l'hypothèse $N \geq 4$) . Restent les deux cas particuliers $u = 0$ , $u = 12^3$ , qui se règlent facilement à l'aide du lemme 2.2, respectivement pour $\tau = \rho$ et $\tau = i$ .

Corollaire.

Soit $Y_o(N)$ un modèle projectif non singulier de $X_o(N)$ . Alors, pour $N \geq 4$ , le paramétrage naturel de $\mathcal{E}_o(N)$ par $Y_o(N)$ (via $J_N$ , et $Y_o(N) \tilde{\to} J_N$) établit une bijection de l'ensemble des points non paraboliques de $Y_o(N)_{\mathbb{Q}}$ sur l'ensemble des classes (à $\mathbb{C}$-isomorphisme près) de couples $(E,R)$ avec $E$ et $R$ rationnels sur $\mathbb{Q}$ .

Démonstration : Il suffit d'appliquer le théorème A , en remarquant que (dans $Y_o(N) \tilde{\to} J_N$) les points paraboliques de $Y_o(N)$ correspondant exactement aux "points à l'infini" de $J_N$ ($u = j(\tau) = \infty$ , $v = j(N\tau) = \infty$) .

Le théorème A (ou plus précisément son corollaire) sera d'un emploi constant au chap. III.

Complément : "modèles de Fricke".

Pour certaines valeurs de $N$ (et notamment les douze valeurs $N = 11$ , $14$ , ..., $49$ mentionnées dans l'introduction), Fricke ([5], vol.II, chap.4) obtient des modèles de $X_o(N)$ plus simples que ceux fournis par les courbes $J_N$ . Pour les valeurs de $N$ qui nous intéressent, ces modèles sont de la forme (*)

$$L_N : y^2 = f(x) \quad ,$$

où $x \in \mathbb{Q}(j, j_N)$ ($j = j(\tau)$ , $j_N = j(N\tau)$) , où $x$ est symétrique en $j$ et $j_N$ , où $y/(j-j_N) \in \mathbb{Q}(x)$ , et où $f(x) \in \mathbb{Q}[x]$ avec $\deg(f) = 3$ ou $4$ . C'est à partir des modèles de Fricke $L_N$ (et non à partir des

(*) Chez Fricke, ces équations s'écrivent $\sigma^2 = f(\tau)$ .

$J_N$ ) que nous calculerons explicitement des $Y_o(N)$ au chap.III.

## II. - Introduction de $Y_1(N)$ .

On peut énoncer, au sujet de $Y_1(N)$ et de $\mathcal{E}_1(N)$ , un résultat analogue au corollaire du théorème A . Toutefois, comme il n'existe, pour $X_1(N)$ , rien d'analogue à $J_N$ , ni au "modèle de Fricke" $L_N$ , il est plus simple de procéder comme Billing et Mahler (dans [1]) : en fait, ces deux auteurs (par des considérations géométriques simples, liées à l'interprétation de la loi de groupe sur une cubique elliptique rappelée au chap. I) construisant (pour tout N) , un modèle projectif (singulier) $B_N$ de $X_1(N)$ , défini sur $\mathbb{Q}$ . Une désingularisation de $B_N$ donne alors un modèle $Y_1(N)$ : une telle désingularisation est faite explicitement dans [1] pour $N = 11$ ; pour $N = 14$ , 15 , voir le chap. IV ci-dessous, ou encore [24] . D'autre part, la construction de Billing et Mahler contient la détermination des points paraboliques de $B_N$ , et le résultat suivant (que nous énonçons ici de façon purement formelle, et par symétrie avec le théorème A) :

Théorème B.

Pour $N \geq 7$ , il existe des bijections "naturelles" entre les trois ensembles suivants :

- l'ensemble $(B_N)_{\mathbb{Q}}$ (privé des points paraboliques) ;
- l'ensemble $\mathcal{E}_1(N)_{\mathbb{Q}}$ ;
- l'ensemble des classes (à $\mathbb{C}$-isomorphisme près) de couples $(E,P)$ avec $E$ et $P$ rationnels sur $\mathbb{Q}$ .

Pour plus amples détails, voir [1] , [16] , notre note [24] , notre exposé [23], et naturellement le chapitre IV. (Signalons également une erreur dans [1] : l'équation correspondant à $N = 14$ , p.41, est inexacte).

# CHAPITRE III

## ETUDE DES COURBES $Y_o(N)$ - APPLICATIONS

On se propose dans ce chapitre de déterminer la valeur $\varepsilon_o(N)$ du cardinal de $\mathcal{E}_o(N)_{\mathbb{Q}}$ pour les 12 valeurs de $N$ tels que $p_o(N) = p(X_o(N)) = 1$ (c'est-à-dire $N = 11,14,15,17,19,20,21,24,27,32,36$ et $49$). Le cardinal $\varepsilon_o(N)$ est fini dans ce cas (voir §2) et par le corollaire du théorème A du chapitre II, on a :

$$\varepsilon_o(N) = \rho_o(N) - \sigma_o(N) \qquad (3,1)$$

où $\rho_o(N)$ = Cardinal de $Y_o(N)_{\mathbb{Q}}$

$\sigma_o(N)$ = Cardinal de l'ensemble de points paraboliques de $Y_o(N)$ rationnels sur $\mathbb{Q}$ .

Il s'agit donc de déterminer $\rho_o(N)$ et $\sigma_o(N)$ ; cela sera fait dans les § 2,3 et 4 .

### §1 - DETERMINATION EFFECTIVE DES MODELES $Y_o(N)$ .

I. - Dans le chapitre II, §4, on a signalé l'existence, pour les 12 valeurs de $N$ telles que $p_o(N) = 1$ -ainsi d'ailleurs que pour d'autres valeurs de $N$ - de modèles affines de $X_o(N)$ du type $L_N$ : $\sigma^2 = f_4(\tau)$ (avec les notations de Fricke : "équations de Fricke"). Dans

la table suivante, nous donnons les équations de ces courbes et les valeurs correspondantes $j_{0,N}$ de l'invariant modulaire j .

TABLE I

| N | Equations de Fricke | $j_{0,N}$ |
|---|---|---|
| 11 | $y^2 = x^4 - 20x^3 + 56x^2 - 44x$ | $-2^{12}.11^{-5}.31^3$ |
| 14 | $y^2 = x^4 - 14x^3 + 19x^2 - 14x + 1$ | $2^{-6}.5^3.7^{-3}.43^3$ |
| 15 | $y^2 = x^4 - 10x^3 - 13x^2 + 10x + 1$ | $3^{-4}.5^{-4}.13^3.37^3$ |
| 17 | $y^2 = x^4 - 6x^3 - 27x^2 - 28x - 16$ | $-3^3.11^3.17^{-3}$ |
| 19 | $y^2 = x^4 - 2^4.x^3 + 2^6.x^2 - 2^2.19x$ | $-2^{18}.7^3.19^{-3}$ |
| 20 | $y^2 = 2x^3 + 13x^2 + 30x + 25$ | $2^4.5^{-2}.11^3$ |
| 21 | $y^2 = x^4 - 6x^3 - 17x^2 - 6x + 1$ | $-2^3.3^{-1}.193$ |
| 24 | $y^2 = x^3 + 11x^2 + 36x + 36$ | $-2^4.3^{-2}.13^3$ |
| 27 | $y^2 = x^4 + 4x^3 + 6x^2 - 3$ | 0 |
| 32 | $y^2 = x^3 + 6x^2 + 16x + 16$ | $2^6.3^3$ |
| 36 | $y^2 = x^3 + 6x^2 + 12x + 9$ | 0 |
| 49 | $y^2 = x^4 - 14x^3 + 63x^2 - 98x + 21$ | $-3^3.5^3$ |

II. - Déterminons maintenant une forme normale de Weierstrass de ces courbes elliptiques. Nous ferons usage pour cela des "formules de Cayley" (voir [5], vol.1, pp. 118-126). Si

$$y^2 = a_o x^4 + 4a_1 x^3 + 6a_2 x^2 + 4a_3 x + a_4$$

est une quartique de genre 1 , et si on pose

$$\begin{aligned} g_2 &= a_o a_4 - 4a_1 a_3 + 3a_2^2 \ , \\ g_3 &= a_o a_2 a_4 + 2a_1 a_2 a_3 - a_o a_3^2 - a_1^2 a_4 - a_2^3 \ ; \end{aligned} \qquad (3,2)$$

alors $y^2 = 4x^3 - g_2 x - g_3$ est un modèle de Weierstrass de la quartique

proposée. Une forme normale de Weierstrass des modèles non-singuliers $Y_o(N)$ obtenue par application des formules (3,2) aux courbes $L_N$ de la table I est ainsi donnée par la table suivante :

TABLE II

| N | Equations normales des $Y_o(N)$ |
|---|---|
| 11 | $y^2 = x^3 - 2^4.3^3.31x - 2^4.3^3.2501$ |
| 14 | $y^2 = x^3 + 3^3.5x - 2.3^3.11.481$ |
| 15 | $y^2 = x^3 - 3^3.481x - 2.3^3.4879$ |
| 17 | $y^2 = x^3 - 11.x - 890$ |
| 19 | $y^2 = x^3 - 2^6.3^3.7x - 2^4.3^3.13.97$ |
| 20 | $y^2 = x^3 + 3^3.11x + 2.3^3.37$ |
| 21 | $y^2 = x^3 - 3^3.193x - 2.3^3.5^2.23$ |
| 24 | $y^2 = x^3 - 3^3.13x + 2.3^3.5.7$ |
| 27 | $y^2 = x^3 + 16$ |
| 32 | $y^2 = x^3 + 4x$ |
| 36 | $y^2 = x^3 + 1$ |
| 49 | $y^2 = x^3 - 35x - 98$ |

III. - Pour certaines valeurs de N ces modèles peuvent être simplifiés ; ainsi, l'existence d'un point rationnel d'ordre 2 sur $Y_o(N)$ permet d'écrire la courbe dans la forme $y^2 = x(x^2+Mx+N)$ . Nous donnons dans la table III les équations simplifiées de $Y_o(N)$ telles qu'elles seront employées dans les § 3 et 4 .

| N | Equations des $Y_o(N)$ |
|---|---|
| 11 | $y^2 = x^3 - 2^4.3^3.31x - 2^4.3^3.2501$ |
| 14 | $y^2 = x(x^2+13x+128)$ |
| 15 | $y^2 = x(x-9)(x-25)$ |
| 17 | $y^2 = x(x^2+30x+289)$ |
| 19 | $y^2 = x^3 - 2^6.3^3.7x - 2^4.3^3.13.97$ |
| 20 | $y^2 = x(x^2-2x+5)$ |
| 21 | $y^2 = x(x-7)(x-16)$ |
| 24 | $y^2 = x(x-3)(x-4)$ |
| 27 | $y^2 = x^3+16$ |
| 32 | $y^2 = x(x^2+4)$ |
| 36 | $y^2 = x^3 + 1$ |
| 49 | $y^2 = x(x^2+21x+112)$ |

## §2 - NULLITE DU RANG DE $Y_o(N)$ .

I. - Il s'agit de voir, pour les 12 valeurs de N faisant l'objet de notre étude, que $Y_o(N)_{\mathbb{Q}}$ est fini. Autrement dit de prouver la

Proposition 3.1.

Si $p_o(N) = 1$ , le rang du $\mathbb{Z}$-module $Y_o(N)_{\mathbb{Q}}$ est 0 .

Nous allons appliquer une méthode élémentaire de descente et nous indiquerons ensuite (remarques III. 1,2,3) les rapports qui existent entre la proposition 3.1 et certaines conjectures "bien connues". La méthode de descente consiste essentiellement en un raisonnement par l'absurde : supposer que le rang n'est pas nul et essayer d'arriver à une contradiction. Voir [1] , [16], [24] .

L'équation de $Y_o(N)$ peut toujours être mise sous la forme :

$$y^2 = (x-e_1)(x-e_2)(x-e_3) \qquad (3,3)$$

dans une extension convenable de $\mathbb{Q}$. Supposons le rang $r \geq 1$ et soit $P(x,y)$ un "point ordinaire générateur" (dans le sens du théorème de Mordell : proposition 1.12). On doit avoir

$$x = A/C^2 \ , \quad y = B/C^3 \ , \quad A,B,C \in \mathbb{Z} \ , \quad (A,C) = (B,C) = 1 \ .$$

De (3,3) , on déduit alors une décomposition

$$A - e_iC^2 = d_iz_i^2 \quad , \quad i = 1,2,3 \qquad (3,4)$$

ou les $d_i$ doivent appartenir a priori à un ensemble fini. Il existe donc un nombre fini de choix pour les triplets $(d_1,d_2,d_3)$ et il suffit de voir que pour chacun d'eux on arrive à une contradiction.

II. - Le procédé est particulièrement simple quand la factorisation (3,3) a lieu dans le corps $\mathbb{Q}$. Cela se vérifie (voir table III) pour $N = 15,21,24$. Pour les valeurs $N = 17,32$ la "division par 2" des équations correspondantes de la table III nous donne (voir la formule (1.7)).

$$N = 17 \qquad y^2 = x(x-1)(x-17)$$

$$N = 32 \qquad y^2 = x(x-1)(x-2) \quad .$$

Le rang étant invariant par isogénie, on peut substituer ces courbes à $Y_o(17)$ , $Y_o(32)$ dans la détermination du $\mathbb{Q}$-rang. La méthode de descente exposée ci-dessus nous donne alors pour les cinq valeurs $\boxed{N = 15,17,21,24,32}$ la valeur $\underline{r(Y_o(N)_{\mathbb{Q}}) = 0}$ .

Examinons à titre d'exemple le cas $N = 21$ :

$$Y_o(21) \ : \ y^2 = x(x-7)(x-16) \quad .$$

La décomposition (3,4) donne

$$A = d_1z_1^2 \quad , \quad A-7C^2 = d_2z_2^2 \quad , \quad A - 16C^2 = d_3z_3^2$$

avec : $d_i, z_i \in \mathbb{Z}$ , $d_i$ sans facteurs carrés, $d_1 . d_2 . d_3$ = un carré et $d_i \mid (e_i - e_j)(e_i - e_k)$ $(i \neq j \neq k \neq i)$ .

On doit donc avoir

$$d_1 = \pm 1, 2, 7 \qquad d_2 = \pm 1, 3, 7 \qquad d_3 = \pm 1, 2, 3 \ .$$

On peut aussi supposer, sans perte de généralité, que $7 \nmid A$ . En effet, il suffit éventuellement de remplacer le point générateur $(x_o, y_o)$ par le point $(x_o y_o) + (0,0) = (x'_o, y'_o)$ . Supposons ce choix fait. On peut également supposer $x_o > 16$ (en prenant si besoin est le nouveau point générateur $(x_o, y_o) + (7,0)$), ce qui implique $d_i > 0$ pour $i = 1,2,3$ .

Il reste alors quatre possibilités :

| | | | | |
|---|---|---|---|---|
| $d_1$ | 1 | 2 | 2 | 1 |
| $d_2$ | 3 | 1 | 3 | 1 |
| $d_3$ | 3 | 2 | 6 | 1 |

Examinons les quatre cas séparément :

a) $A = z_1^2$ , $A - 7C^2 = 3z_2^2$ , $A - 16C^2 = 3z_3^2$ .

Comme $(A,C) = 1$ , la considération de la deuxième équation modulo 4 nous mène à une contradiction.

b) $A = 2z_1^2$ , $A - 7C^2 = z_2^2$ , $A - 16C^2 = 2z_3^2$ .

A est divisible par 8 . En effectuant une division par 8 dans la troisième équation, on la ramène à la forme : $z^2 - 2C^2 = z_3^2$ , et, modulo 4, on obtient une contradiction.

c) $A = 2z^2$ , $A - 7C^2 = 3z_2^2$ , $A - 16C^2 = 6z^2$ .

A est divisible par 2, mais non par 4, et la troisième équation conduit, en réduisant modulo 4, à une contradiction.

d) $A = z^2$ , $A - zC^2 = z_2^2$ , $A - 16C^2 = z^2$ .

Dans ce cas, on a (voir [12], chap.16, th.6) l'égalité $(x_o,y_o) = 2(x'_o,y'_o)$ , en contradiction avec le caractère générateur de $(x_o,y_o)$ .

III. - Pour $\boxed{N = 14,20,36,49}$ les courbes $Y_o(N)$ admettent une factorisation du type (3,3) dans les corps quadratiques $\mathbb{Q}(\sqrt{-7})$ , $\mathbb{Q}(\sqrt{-1})$ , $\mathbb{Q}(\sqrt{-3})$ et $\mathbb{Q}(\sqrt{-7})$ respectivement. Ces corps sont principaux et à groupe d'unités fini. On peut alors raisonner dans ces corps comme on l'a fait ci-dessus dans $\mathbb{Q}$ . Voyons par exemple le cas $N = 20$ .

$$Y_o(20) : y^2 = x(x^2-2x+5) = x(x-1-2i)(x-1+2i) .$$

La décomposition (3,4) donne maintenant

$$A = d_1z_1^2 \quad , \quad A - (1+2i)C^2 = d_2z_2^2 \quad , \quad A - (1-2i)C^2 = d_3z_3^2 \quad ,$$

avec

$$d_1 \mid 5 = \mathfrak{p}_1\mathfrak{p}_2 \quad , \quad d_2 \mid 4(-2+i) = 4\mathfrak{p}_1 \quad , \quad d_3 \mid 4(-2-i) = 4\mathfrak{p}_2 \quad .$$

Sans perte de généralité, on peut supposer $\mathfrak{p}_1 \nmid d_1$ et $\mathfrak{p}_2 \nmid d_1$ .

Les unités de $\mathbb{Q}(i)$ sont : $\pm 1$ , $\pm i$ . Compte tenu du fait que $-1$ est un carré, il reste les possibilités :

$$d_1 = 1,i \quad , \quad d_2 = 1,i,i+1,i-1 \quad , \quad d_3 = 1,i,i+1,i-1 \quad ,$$

avec $(i+1)^2 = (2)$ ; d'où huit cas :

| $d_1$ | 1 | 1 | 1 | i | i | i | i | 1 |
|---|---|---|---|---|---|---|---|---|
| $d_2$ | i | i+1 | i-1 | i | 1 | i+1 | i-1 | 1 |
| $d_3$ | i | i+1 | i-1 | 1 | i | i+1 | i-1 | 1 |

Dans tous les cas, on arrive à une contradiction par des considérations de congruences. Voyons le premier cas ; on aura :

$$A = z_1^2 = (a_1+b_1 i)^2 \quad ,$$
$$A - (1+2i)C^2 = iz_2^2 = i(a_2+b_2 i)^2 \quad ,$$
$$A - (1-2i)C^2 = iz_3^2 = i(a_3+b_3 i)^2 \quad .$$

Ceci implique :

$$a_1.b_1 = 0 \quad , \quad a_1^2 - b_1^2 = A \quad , \quad -2a_2b_2 = A - C^2 \quad , \quad a_2^2 - b_2^2 = -2C^2 \quad .$$

Si $a_1 = 0$ , $A = -b_1^2$ . Compte tenu de $(A,C) = 1$ , et en prenant modulo 4 dans la troisième équation, on voit que la seule possibilité est que $A$ et $C$ soient impairs. Mais si $C$ est impair, la quatrième équation, réduite modulo 8, conduit à une contradiction. Si $b_1 = 0$ , $A = a_1^2$ . De la troisième équation, réduite modulo 4, on déduit encore que $A$ et $C$ sont impairs, et on applique le même raisonnement qu'avant.

IV. - Il reste les trois valeurs $\boxed{N = 11,19,27}$ .

a) Pour $N = 11$ , la nullité du $\mathbb{Q}$-rang de $Y_o(N)$ résulte de [1] . En effet, $Y_o(11)$ et $Y_1(11)$ sont $\mathbb{Q}$-isogènes, et Billing et Mahler prouvent dans [1] (par décomposition du type (3,3) dans un corps cubique principal) que $r(Y_1(11)_{\mathbb{Q}}) = 0$ . Ainsi : $\underline{r(Y_o(11)_{\mathbb{Q}}) = 0}$ (voir d'ailleurs la remarque 1 ci-dessous, ainsi que le chapitre IV).

b) Pour $N = 27$ , $Y_o(N)$ s'écrit $y^2 = x^3 + 16$ . C'est une courbe du type $y^2 = x^3 + k$ , largement étudié dans la littérature (Mordell, Nagell, Selmer, Cassels,...). La table de Selmer ([19], p. 285, $D = -k = -16$) montre que $Y_o(27)_{\mathbb{Q}}$ n'a pas de générateurs d'ordre infini. Ainsi, $\underline{r(Y_o(27)_{\mathbb{Q}}) = 0}$ .

c) Pour $N = 19$ enfin, on est dans un cas "difficile" : pour la courbe $Y_o(19)$ , en effet, la décomposition (3,3) se fait dans le corps des racines du polynôme $x^3 - 2^6.3^3.7.x - 2^4.3^3.13.97$ , dont l'arithmétique ne semble présenter aucune particularité susceptible de simplifier les

calculs. On peut toutefois prouver la nullité de $r(Y_o(19)_{\mathbb{Q}})$ en utilisant les résultats de Mazur [29 ] , notamment le th. (3,5), p. 56 : ce théorème implique en effet l'inégalité

$$r(Y_o(19)_{\mathbb{Q}}) \leq a + m - 1 \quad ,$$

où $m$ est le nombre de points de mauvaise réduction de $Y_o(19)$ [soit $m = 1$ , puisque $Y_o(19)$ a bonne réduction hors de $\{19\}$ ] et où $a$ est le nombre de points de réduction de type additif pour $Y_o(19)$ [soit $a = 0$ , puisque la mauvaise réduction de $Y_o(19)$ en 19 est de type multiplicatif : voir par exemple [9] , p.9 ] ; ainsi, $r(Y_o(19)_{\mathbb{Q}}) \leq 1 + 0 - 1$ , donc $\underline{r(Y_o(19)_{\mathbb{Q}}) = 0}$ .

V. - Remarque 1. Le revêtement $X_1(N) \to X_o(N)$ induit une application rationnelle $\lambda : Y_1(N) \to Y_o(N)$ , définie sur $\mathbb{Q}$ . Si $Y_1(N)$ et $Y_o(N)$ sont de genre 1 (cela se produit pour $N = 11,14,15$) , $\lambda$ est une $\mathbb{Q}$-isogénie. Donc $Y_o(N)_{\mathbb{Q}}$ et $Y_1(N)_{\mathbb{Q}}$ ont le même rang. Billing et Mahler ont montré (voir [1]) que le rang de $Y_1(11)_{\mathbb{Q}}$ est 0 , ce qui (comme on l'a vu plus haut) implique que le rang de $Y_o(11)_{\mathbb{Q}}$ est aussi 0 . Le même argument est valable pour $N = 15$ (voir [24]). Signalons que pour $N = 17$ , Ogg (voir [16]) a montré qu'une certaine courbe isogène à $Y_o(17)$ a pour $\mathbb{Q}$-rang 0 .

Remarque 2. Les conjectures de Birch et Swinnerton-Dyer (voir [21]) impliquent que le rang de $Y_o(N)_{\mathbb{Q}}$ est nul, et donc que $\rho_o(N)$ est fini pour les 12 valeurs de $N$ étudiées ici. Cette propriété a été vérifiée directement dans ce contexte par Birch (voir [20] pp. 182 et 221) et Ligozat [9].

## §3 - CALCUL DE $\rho_o(N)$ .

I. - On a montré au §2 que $Y_o(N)_{\mathbb{Q}}$ se réduit à sa partie de torsion, c'est-à-dire à ses points exceptionnels. Ceux-ci peuvent être calculés explicitement (à partir des équations normales de Weierstrass

des $Y_o(N)$ : table II) par application de la proposition 1.12 . En effet, il suffit d'essayer comme valeurs possibles de l'ordonnée d'un point exceptionnel $P$ , la valeur 0 et les entiers rationnels dont le carré est un diviseur du discriminant de $Y_o(N)$ . Les calculs peuvent être longs ; les remarques suivantes aident à les simplifier.

i) Si on connaît les points exceptionnels $P_1,\ldots,P_n$ de $Y_o(N)_{\mathbb{Q}}$, les points $P_i+P_j$ , $i,j = 1,\ldots,n$ , sont également rationnels et exceptionnels, et peuvent être obtenus par la méthode de "tangente et corde" (voir chap.I, prop. 1,3, corollaire).

ii) Nagell [14], Lind [10] donnent des conditions à remplir par les coefficients $A$ , $B$ de la courbe

$$E : y^2 = x^3 - Ax - B$$

pour qu'elle puisse admettre un groupe de torsion d'une structure donnée.

iii) Si la courbe admet une bonne réduction modulo deux nombres premiers différents $p$ , $q$ , et si le nombre $N(q)$ d'éléments de la courbe réduite $\tilde{Y}_o(N)$ rationnels sur $\mathbb{F}_q$ est premier à $p$ , la proposition 1.13 est applicable : $\rho_o(N)$ doit alors être un diviseur du nombre $N(p)$ .

Dans la table suivante nous faisons figurer les résultats obtenus pour les courbes $Y_o(N)$ dans la forme figurant dans la table III . La dernière colonne indique la structure de $Y_o(N)_{\mathbb{Q}}$ .

TABLE IV

| N | Points | $\rho_o(N)$ | structur |
|---|---|---|---|
| 11 | $(\infty)$ , $(2^3.3.7, \pm 2^2.3^3.11)$ , $(2^2.3.47, \pm 2^2.3^3.11^2)$ | 5 | $C_5$ |
| 14 | $(\infty)$ , $(0,0)$ , $(2^2, \pm 2^2.7)$ , $(2^5, \pm 2^5.7)$ | 6 | $C_6$ |
| 15 | $(\infty)$ , $(0,0)$ , $(9,0)$ , $(5^2,0)$ , $(5, \pm 2^2.5)$ , $(3^3.5, \pm 2^2.3^2.5)$ | 8 | $C_2 \times C_4$ |
| 17 | $(\infty)$ , $(0,0)$ , $(17, \pm 2^3.17)$ | 4 | $C_4$ |
| 19 | $(\infty)$ , $(2.3, \pm 2^2.3^3.19)$ | 3 | $C_3$ |
| 20 | $(\infty)$ , $(0,0)$ , $(1, \pm 2)$ , $(5, \pm 2.5)$ | 6 | $C_6$ |
| 21 | $(\infty)$ , $(0,0)$ , $(7,0)$ , $(2^4,0)$ , $(2^2, \pm 2^2.3)$ , $(2^2.7, \pm 2^2.3.7)$ | 8 | $C_2 \times C_4$ |
| 24 | $(\infty)$ , $(0,0)$ , $(3,0)$ , $(2^2,0)$ , $(2, \pm 2)$ , $(2.3, \pm 2^2.3)$ | 8 | $C_2 \times C_4$ |
| 27 | $(\infty)$ , $(0, \pm 2^2)$ | 3 | $C_3$ |
| 32 | $(\infty)$ , $(0,0)$ , $(2, \pm 2^2)$ | 4 | $C_4$ |
| 36 | $(\infty)$ , $(-1,0)$ , $(0, \pm 1)$ , $(2, \pm 3)$ | 6 | $C_6$ |
| 49 | $(0,0)$ , $(\infty)$ | 2 | $C_2$ |

## §4 - DETERMINATION DE $\sigma_o(N)$ .

I. - La formule (2,2) nous donne le nombre total de points paraboliques $P_{d,i}$ de $Y_o(N)$ . Le diviseur parabolique $\Delta_o(N)$ étant rationnel, les points $P_{d,i}$ appartiennent à une certaine extension algébrique de $\mathbb{Q}$ . Il s'agit de voir lesquels d'entre eux sont rationnels (sur $\mathbb{Q}$) . On va donner deux méthodes élémentaires permettant de résoudre le problème pour certaines valeurs de N . Ces méthodes sont esquissées dans la note [8] .

i) L'application $\xi : X_o(N) \to J_N$ définie par : $\tau \to (j(\tau), j(N\tau))$ applique les points paraboliques de $X_o(N)$ sur les points à l'infini de $J_N$ (*). Il s'agit donc de voir lesquels parmi ces points sont rationnels ; cela est possible pour des petites valeurs de N pour lesquels on a une

(*) Ces points à l'infini seront évidemment dits "paraboliques".

uniformisation explicite du corps $K_N = \mathbb{Q}(j, j_N)$ . Voir II.

ii) $\Delta_o(N)$ étant rationnel, il est invariant par $G = \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ : pour tout $\sigma \in G$ , $\Delta_o(N)^\sigma = \Delta_o(N)$ . Autrement dit :

$$\sum_{d|N} d/t(P^\sigma_{d,1}+\ldots+P^\sigma_{d,\varphi(t)}) = \sum_{d|N} d/t(P_{d,1}+\ldots+P_{d,\varphi(t)}) \ . \qquad (3,5)$$

Cette simple remarque donne la valeur $\sigma_o(N)$ pour $N$ sans facteurs carrés, et des indications intéressantes pour d'autres valeurs de $N$ . Voir III.

D'autres valeurs de $N$ peuvent être étudiées par la combinaison des méthodes i) et ii) . Voir IV.

II. - Pour l'obtention d'une uniformisation de $K_N$ , nous ferons usage de résultats de Fricke ([5], Vol. II, Chap.IV).

Commençons par examiner le cas où $p_o(N) = 0$ . Nous développerons en détail les calculs pour les valeurs de $N$ qui nous seront nécessaires par la suite, nous limitant pour les autres à indiquer la valeur de $\sigma_o(N)$ obtenue.

**N = 4** . De [5] , p. 374, on déduit :

$$j = 64\,\frac{(t^2+8t+4)^3}{t^4(2t+1)} \quad , \qquad j_4 = 8\,\frac{(64t^2+32t+1)^3}{t(1+2t)} \ .$$

Les points paraboliques de $J_4$ correspondent aux valeurs $t = \infty, 0, 1/2$ , et sont donc tous trois rationnels. D'où $\sigma_o(4) = 3$ .

**N = 8** . De [5] , p. 325, on déduit :

$$j = 2^8\,\frac{f_{12}(t)}{t(t+4)(t+2)^2} \quad , \qquad j_8 = 2\,\frac{f_{12}(t)}{t^8(t+2)(t+4)^2}$$

$f_n$ désignant ici un polynôme de degré $n$ à coefficients dans $\mathbb{Z}$ .
Les quatre points paraboliques correspondent à $t = \infty$ , $0$ , $-1/2$ , $-1/4$ et sont donc rationnels : $\sigma_o(8) = 4$ .

$\boxed{N = 16}$ . De [5] , p. 377, on déduit :

$$j = \frac{f_{24}(t)}{t(t+4)(t+2)^4(t^2+4t+8)} \quad , \quad j_{16} = \frac{f_{24}(t)}{2^8 t^{16}(t+2)(t+4)^4(t^2+4t+8)} \quad .$$

Quatre points paraboliques (ceux qui correspondent aux valeurs $t = \infty$ , $0$ , $-1/4$ , $-1/2$) sont rationnels, les deux autres étant définis sur $\mathbb{Q}(i)$ : $\sigma_o(16) = 4$ .

$\boxed{N = 9}$ . De [5] , p. 387, on déduit :

$$j = 3^3 \frac{f_{12}(t)}{t(t^4+3t+3)} \quad , \quad j_9 = \frac{f_{12}(t)}{t^9(3+3t+t^2)} \quad .$$

Les deux points paraboliques correspondant à $t = \infty$ , $0$ sont rationnels, les deux restants étant définis sur $\mathbb{Q}(\sqrt{-3})$ : $\sigma_o(9) = 2$ .

Résumons maintenant les résultats pour les 15 valeurs de $N$ tels que $p_o(N) = 0$ .

TABLE V

| $N$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 12 | 13 | 16 | 18 | 25 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $\sigma_o(N)$ | 1 | 2 | 2 | 3 | 2 | 4 | 2 | 4 | 2 | 4 | 6 | 2 | 4 | 4 | 2 |

Quand $p_o(N) = 1$ , $j$ et $j_N$ admettent un paramétrage rationnel comme fonction de deux paramètres $t,s$ liés par une équation de genre 1.(*) Voyons quelques exemples.

(*) Chez Fricke, $t$ et $s$ sont notés $\tau$ et $\sigma$ .

$\boxed{N = 32}$ . De [5] , p. 379, on déduit :

$$j = \frac{f_{24}(t)}{t(t+4)(t+2)^4(t^2+4t+8)} \quad , \quad j_{32} = \frac{f_{48}(t,s)}{t^{32} f_{15}(t,s)} \quad ,$$

avec $s^2 = t^3 + 6t^2 + 16t + 16$ . Il y a quatre points paraboliques rationnels en correspondance avec les valeurs de $t = \infty$ , $0$ , $-1/4$ , $-1/2$ : $\sigma_o(32) = 4$ .

$\boxed{N = 27}$ . De [5] , pp. 388-9 , on déduit :

$$j = \frac{f_{12}(t)}{t(t^2+3t+3)} \quad , \quad j_{27} = \frac{f_{12}(t,s)}{f_{12}(t,s)} \quad ,$$

avec $s^3 = q(t^2+3t+3)$ . Il y a deux points paraboliques rationnels pour $t = \infty$ , $0$ : $\sigma_o(27) = 2$ .

$\boxed{N = 49}$ . De [5] , p. 402, on déduit :

$$j = \frac{f_8(t)}{t} \quad , \quad j_{49} = \frac{f_{32}(t,s)}{t.s^{28}} \quad ,$$

avec $t^2 - 7^3.t(s+5s^2+7s^3) - 7^4(s+7s^2+3.7s^3+7^2s^4+3.7^2s^5+7^3s^6+7^3s^7) = 0$ . Les deux seuls points paraboliques rationnels correspondent aux valeurs $t = \infty$ , $0$ : $\sigma_o(49) = 2$ .

III. - De la formule (3,5) on déduit sans peine :

Proposition 3.2.

*Soit* $N$ *sans facteurs carrés*, $N = p_1.....p_n$ . *Les* $2^n$ *points paraboliques de* $Y_o(N)$ *sont alors tous rationnels ; autrement dit* $\sigma_o(N) = 2^n$ .

Démonstration : Ceci résulte de la remarque générale suivante : soit $d|N$ pour lequel $\varphi(t) = 1$ , et supposons que le coefficient $d/t$ figure une seule fois dans $\Delta_o(N)$ : alors le point $P_{d,1}$ est rationnel.

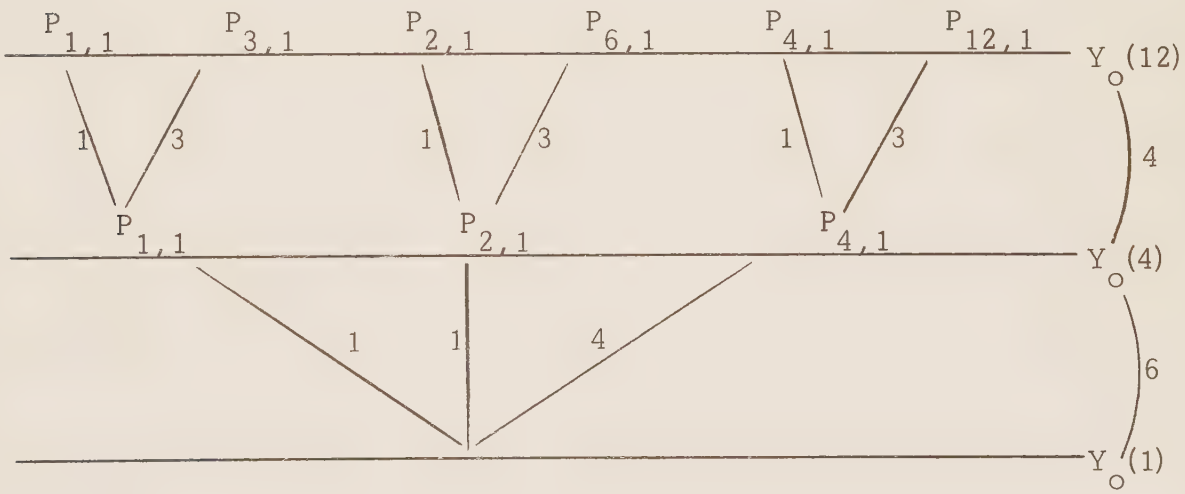
IV. - On va "raffiner" la méthode ii) en prenant un diviseur "convenable" $N'$ de $N$ et en considérant le double revêtement

$$J(N) \xrightarrow{\pi_{N,N'}} J(N') \xrightarrow{\pi_{N'}} J(1) \quad .$$

Le "revêtement relatif" $\pi_{N,N'}$ est défini sur $\mathbb{Q}$ (comme on peut le déduire de l'inclusion $\mathbb{Q}(j,j_{N'}) \subset \mathbb{Q}(j,j_N)$) . Si les points paraboliques rationnels de $J_{N'}$ sont connus (par exemple, par application de la méthode i)) , il suffit alors d'étudier la décomposition de $\Delta_o(N')$ dans le revêtement $\pi_{N,N'}$ .

Exemples.

$\boxed{N = 12}$ . Prenons $N' = 4$ . Alors $N/N' = 3$ . On a le diagramme de décomposition suivant :




Les trois points paraboliques de $Y_o(4)$ étant rationnels, il en est de même des trois diviseurs partiels de $\Delta_o(12)$

$$P_{11} + 3P_{3,1} \qquad P_{2,1} + 3P_{6,1} \qquad 4P_{4,1} + 12P_{12,1} \ ;$$

le raisonnement de la proposition 3.2 nous donne alors : $\sigma_o(12) = 6$ .

$\boxed{N = 24}$ . $N' = 8$ , $N/N' = 3$ .

Les quatre points paraboliques de $Y_o(8)$ étant rationnels, on a de façon analogue au cas antérieur, $\sigma_o(24) = 8$ .

$\boxed{N = 48}$ . $N' = 16$ , $N/N' = 3$ .

Quatre points paraboliques de $Y_o(16)$ sont rationnels ; on en déduit immédiatement la rationalité des 8 points paraboliques de $Y_o(48)$ dans lesquels ils se décomposent.

Généralisons ces résultats.

Proposition 3.3.

Soit N tel que $N' = 4$ divise N (resp. $N' = 8$ , 16 divise N) et tel que $(N/N', 2) = 1$ , $N/N' = p_1 \ldots p_n$ , les $p_i$ premiers distincts. Alors $\sigma_o(N) = 3.2^n$ (resp. $4.2^n, 8.2^n$) . .

De même, on peut démontrer :

Proposition 3.4.

Soit N tel que $9/N$ , $(N/9 , 3) = 1$ , $N/9 = p_1 \cdot \ldots \cdot p_n$ . Alors $\sigma_o(N) = 2.2^n = 2^{n+1}$ .

V. - Les résultats de II , III et IV nous permettent d'obtenir la valeur $\sigma_o(N)$ pour les 12 valeurs de N telles que $\rho_o(N) = 1$ . Nous avons ainsi la table suivante :

TABLE VI

| N | 11 | 14 | 15 | 17 | 19 | 20 | 21 | 24 | 27 | 32 | 36 | 49 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $\sigma_o(N)$ | 2 | 4 | 4 | 2 | 2 | 6 | 4 | 8 | 2 | 4 | 6 | 2 |

Remarque.

En fait, d'après Ogg [17], on peut prouver plus généralement (avec nos notations) que les points paraboliques $P_{d,i}$ sont rationnels sur le corps $\mathbb{Q}(e^{2\pi i/t})$ . En particulier, sont rationnels les points qui correspondent à un $d$ pour lequel $\varphi(t) = 1$ (c'est-à-dire $t = 1,2$) . Les résultats obtenus par application de i) et ii) sont évidemment compatibles avec cet énoncé.

## §5 - ETUDE DE $\mathcal{E}_o(N)_{\mathbb{Q}}$ . CONCLUSION.

I. - La formule (3,1) et les tables IV et VI donnent la table suivante :

TABLE VII

| N | 11 | 14 | 15 | 17 | 19 | 20 | 21 | 24 | 27 | 32 | 36 | 49 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $\epsilon_o(N)$ | 3 | 2 | 4 | 2 | 1 | 0 | 4 | 0 | 1 | 0 | 0 | 0 |

Proposition 3.5.

Pour $N = 20 , 24 , 32 , 36 , 49$ , l'ensemble $\mathcal{E}_o(N)_{\mathbb{Q}}$ est vide.

Compte tenu de la définition de $\epsilon_o(N)$ (chap. II, §.3,I) , on a donc

Théorème A.

Il n'existe aucune courbe elliptique définie sur $\mathbb{Q}$ ayant un sous-groupe cyclique rationnel sur $\mathbb{Q}$, et d'ordre $N = 20 , 24 , 32 , 36 , 49$ .

II. - Courbes à multiplication complexe.

Nous allons maintenant voir que certains des éléments de $\mathcal{E}_o(N)_{\mathbb{Q}}$ sont formés par une courbe à multiplication complexe $E$ et le noyau $R$ d'une multiplication complexe de $E$ .

Soit $E$ une courbe elliptique (définie sur $\mathbb{C}$), à multiplication complexe, associée au réseau $\Lambda$ (chap. I, §2) de base $(\tau,1)$ , d'anneau d'endomorphismes $\mathrm{End}(E)$ égal à $O_f$ , l'ordre de conducteur $f$ dans l'anneau des entiers $A$ du corps quadratique $K = \mathbb{Q}(\tau)$ . La formule (2,8) nous donne le degré $h_f$ de l'extension $K(j_E)/K$ . Pour que $E$ soit définie sur $\mathbb{Q}$ , il est évidemment nécessaire que $h_f = 1$ .

Pour $N = 14 , 15 , 17 , 21$ , il est facile de voir que les courbes elliptiques de $\mathcal{E}_o(N)_{\mathbb{Q}}$ n'admettent pas de multiplication complexe de degré $N$ . En effet, une telle courbe devrait avoir comme réseau $(\sqrt{-N},1)$ ou $((1+\sqrt{-N})/2,1)$ et l'application de la formule (2,4) montre que dans ces cas $h_f > 1$ . Une telle courbe ne saurait donc être définie sur $\mathbb{Q}$ . Cette remarque explique la parité de $\varepsilon_o(N)$ pour ces quatre valeurs de $N$ .

Par contre pour $\boxed{N = 11 , 19}$ nous pouvons considérer les courbes elliptiques dont le réseau associé est l'anneau des entiers des corps $\mathbb{Q}(\sqrt{-11})$ et $\mathbb{Q}(\sqrt{-19})$ , pour lesquels la formule (2,8) montre qu'on a $h_f = 1$ . La condition nécessaire est donc vérifiée. En fait, les invariants $j$ de ces courbes (qui ont été calculés par Weber, [27], vol. 3, §125) sont rationnels, et on a

pour $N = 11$ , $j = -2^{15}$ (courbe $E_{11}$) ;

pour $N = 19$ , $j = -2^{15}.3^3$ (courbe $E_{19}$) ;

$E_{11}$ (resp. $E_{19}$) possède des multiplications complexes par les entiers de $\mathbb{Q}(\sqrt{-11})$ (resp. $\mathbb{Q}(\sqrt{-19})$). En particulier, elle admet la multiplication complexe par $\alpha = \sqrt{-11}$ (resp. $\sqrt{-19}$), et le noyau de $\alpha$, $R_{11}$ (resp. $R_{19}$), est cyclique d'ordre 11 (resp. 19) engendré par le point d'argument elliptique $1/\sqrt{-11}$ (resp. $1/\sqrt{-19}$).

Pour $\boxed{N = 27}$, considérons de même le réseau $(\frac{1+3\sqrt{-3}}{2}, 1)$ ordre de conducteur 3 dans l'anneau des entiers du corps principal $\mathbb{Q}(\sqrt{-3})$. Soit $E_{27}$ la courbe elliptique associée à ce réseau ; son invariant $j$ est rationnel et a pour valeur $j = -2^{15}.3.5^3$. (Weber, op. cit.). La courbe $E_{27}$ admet la multiplication complexe par $\sqrt{-27}$, dont le noyau, $R_{27}$, est un groupe cyclique rationnel sur $\mathbb{Q}$ d'ordre 27, engendré par $1/\sqrt{-27}$.

Proposition 3.6.

*Le seul élément de* $\mathcal{E}_o(N)_{\mathbb{Q}}$ *pour* $N = 19$ (*resp.* 27) *est* $(E_{19}, R_{19})$ (*resp.* $(E_{27}, R_{27})$). *Pour* $N = 11$, $(E_{11}, R_{11})$ *est l'un des trois éléments de* $\mathcal{E}_o(11)_{\mathbb{Q}}$.

III. - Isogénies.

L'ensemble $\mathcal{E}_o(11)_{\mathbb{Q}}$ possède trois éléments, l'un d'eux correspondant à la courbe $E_{11}$ d'invariant $j = -2^{15}$. Appelons $(E'_{11}, R'_{11})$ et $(E''_{11}, R''_{11})$ les deux autres éléments. Les courbes $E'_{11}$ et $E''_{11}$ sont liées par une isogénie de degré 11. En effet, soit $\lambda : E'_{11} \to E''_{11}$ l'isogénie correspondant à la division par $R'_{11}$ (chap. I, proposition 1.5) et soit $\hat{\lambda}$ l'isogénie duale, $R'''_{11}$ le noyau de $\hat{\lambda}$. Alors $(E'''_{11}, R'''_{11}) \in \mathcal{E}_o(11)_{\mathbb{Q}}$ et donc $((E'''_{11}, R'''_{11})) = ((E''_{11}, R''_{11}))$.

Vélu [25] a obtenu les invariants $j$ des courbes $E'_{11}$ et $E''_{11}$ : $-11^2$ et $-11.131^3$ respectivement.

Résumons ces résultats :

Théorème B.

Les trois classes de courbes elliptiques définies sur $\mathbb{Q}$ et ayant un sous-groupe cyclique rationnel d'ordre 11 rationnel sur $\mathbb{Q}$ sont celles d'invariants modulaires

$$j = -2^{15} \quad , \quad j = -11^2 \quad , \quad j = -11.131^3 \quad .$$

La seule classe de courbes ayant un sous-groupe cyclique rationnel sur $\mathbb{Q}$ d'ordre 19 (resp. 27) a comme invariant modulaire $j = -2^{15}.3^3$ (resp. $-2^{15}.3.5^3$) .

Par un raisonnement analogue à celui employé ci-dessus on a :

Proposition 3.7.

Les 2 éléments de $\mathcal{E}_o(N)_{\mathbb{Q}}$ pour $N = 14 , 17$ sont liés par une $\mathbb{Q}$-isogénie de degré 14 et 17 respectivement. Les 4 éléments pour $N = 15 , 21$ sont liés deux par deux par des $\mathbb{Q}$-isogénies d'ordre 15 et 21 respectivement.

## §6 - APPLICATIONS.

Les résultats du §5 (table VII) permettent de donner des indications sur le cardinal $\epsilon_1(N)$ de l'ensemble $\mathcal{E}_1(N)_{\mathbb{Q}}$ pour certaines valeurs de $N$ . Faisons en effet, la remarque triviale qu'un point $P$ d'ordre $N$ rationnel sur $\mathbb{Q}$ sur une courbe elliptique engendre un groupe cyclique $R$ d'ordre $N$ rationnel sur $\mathbb{Q}$ . On déduit alors du théorème A :

Théorème C.

Il n'existe aucune courbe elliptique définie sur $\mathbb{Q}$ ayant un point rationnel d'ordre $N = 20 , 24 , 32 , 36 , 49$ .

On va voir que le même résultat est encore vrai pour $\boxed{N = 19 \ , \ 27}$. Pour ces valeurs de $N$ le seul élément de $\mathcal{C}_o(N)_{\mathbb{Q}}$ correspond à une courbe à multiplication complexe, le sous-groupe cyclique étant le noyau de la multiplication complexe par $\sqrt{-19}$ et $\sqrt{-27}$ respectivement. Il suffit de voir qu'un point générateur de ce sous-groupe n'est pas rationnel. On fera usage pour cela de la théorie de la multiplication complexe (voir [7]). Le cas $N = 19$ ayant été traité dans notre note [7], voyons ici le cas $N = 27$.

Appelons $\pi$ la multiplication complexe par $\sqrt{-27}$, le sous-groupe $R_{27}$ (voir proposition 3.7) est engendré par le point d'argument elliptique $u = 1/\sqrt{-27}$ (c'est-à-dire par le point $(x(u),y(u))$. Soient $K = \mathbb{Q}(\sqrt{-3})$, corps principal à groupe des unités $\{\pm 1, \pm\rho, \pm\rho^2\}$, $L = K(X(u))$, $J_K$ le groupe des idèles de $K$, $M$ l'ensemble des places non-archimédiennes de $K$, $K_\mathfrak{p}$ le complété de $K$ pour la place $\mathfrak{p} \in M$ ; soient $U_\mathfrak{p}$ le groupe des unités de $K_\mathfrak{p}$ et $U_\mathfrak{p}^{(n)}$ le sous-groupe des unités congrues à 1 modulo $\mathfrak{p}^n$. Soient finalement :

$$V = \{s \in J_K \mid s_\mathfrak{p} \in U_\mathfrak{p} \text{ pour toute } \mathfrak{p} \in M\} \ ,$$

$$W = \{s \in V \ ; \ s_{(\sqrt{-3})} \in U^{(3)}_{(\sqrt{-3})}\} \ .$$

Le théorème fondamental de la multiplication complexe (voir [20], th. 5.5) nous montre alors que $L$ est le sous-corps de $K_{ab}$ correspondant à $K^*W$. Il suffit ici de voir que l'extension $L/K$ n'est pas triviale. Mais, $K$ étant principal,

$$G(L/K) \simeq J_K/K^*W = K^*V/K^*W \simeq V/(K^*W)\cap V = \frac{V}{\{\pm 1\}.W} \simeq U_{\sqrt{-3}}/\{\pm 1\}.U^{(3)}_{\sqrt{-3}}$$

$$\simeq \mathbb{F}_3^+ \times \mathbb{F}_3^\times \times \mathbb{F}_3^\times/\{\pm 1\} \ ,$$

et effectivement, $L/K$ est une extension de degré 9.

Du théorème B et de ce résultat on déduit alors :

Théorème D.

Il n'existe aucune courbe elliptique définie sur $\mathbb{Q}$ ayant un point rationnel sur $\mathbb{Q}$ d'ordre 19 ou 27.

# CHAPITRE IV

## ETUDE DES COURBES $Y_1(N)$ . APPLICATIONS

Soit $Y_1(N)$ un modèle projectif non-singulier de la surface de Riemann $X_1(N)$ . Soit $\varepsilon_1(N) = \mathrm{card}(\mathcal{E}_1(N)_{\mathbb{Q}})$ . Par le théorème 2.2, on a :

$$\varepsilon_1(N) = \rho_1(N) - \sigma_1(N) \qquad (4,1)$$

où $\rho_1(N)$ = nombre de points de $Y_1(N)$ rationnels sur $\mathbb{Q}$ ;
$\sigma_1(N)$ = nombre de points paraboliques de $Y_1(N)$ rationnels sur $\mathbb{Q}$ .

Ogg [16] a émis la conjecture selon laquelle $\mathcal{E}_1(N)_{\mathbb{Q}}$ est vide sauf pour les valeurs de $N$ telles que $p_1(N) = p(X_1(N)) = 0$ . Cette conjecture est vérifiée pour les 11 valeurs $N = 1\text{-}10$ et 12 pour lesquelles $\mathcal{E}_1(N)_{\mathbb{Q}}$ est infini : en effet, pour ces valeurs de $N$ , $p_1(N) = 0$ (et ce sont d'ailleurs les seules) ; et d'autre part, il existe une infinité de courbes elliptiques admettant un point rationnel d'ordre $N = 1\text{-}10$ ou 12 . Voir par exemple [10].

Ici, on se propose d'étudier les valeurs $\boxed{N = 11,14,15}$ , c'est-à-dire les valeurs de $N$ telles que $p_1(N) = 1$ . On montrera, en accord avec la conjecture d'Ogg , que dans ces cas, $\varepsilon_1(N) = 0$ . On rappelle (voir l'introduction) que cette conjecture a été vérifiée récemment par Ogg [16] , pour $\boxed{N = 17}$ ; par Ogg-Mazur [17] , pour $\boxed{N = 13,18}$ ; par Mazur-Vélu, [31], pour $\boxed{N = 26}$(*) ; par Swinnerton-Dyer [21], pour $\boxed{N = 37}$ (voir d'ailleurs le §3 ci-dessous, "Remarques"). Nos résultats du chapitre III confirment cette conjecture pour $\boxed{N = 19,27,32,36,49}$ .

---

(*) Le cas "N = 26" peut évidemment se déduire du cas "N = 13" .

L'égalité $\varepsilon_1(N) = 0$ pour $\boxed{N = 16,20,24}$ était déjà connue de Nagell [14] . Enfin, Hellegouarch vient de la démontrer pour $\boxed{N = 2p^2}$ (p premier $\geq 5$) , donc pour $\boxed{N = 50,98,\ldots}$ : voir [28] .

## §1 - DETERMINATION EFFECTIVE DE $Y_1(N)$ .

I. - Dans le chapitre II, on a vu comment une méthode, due à Billing et Mahler [1] permet d'obtenir un modèle projectif $B_N$ de $X_1(N)$ . Pour les trois valeurs $N = 11 , 14 , 15$ ces équations sont

$$\begin{aligned} N = 11 &: \quad x_1^2x_2 - x_1x_2^2 - x_1x_3^2 + x_2^2x_3 = 0 \ ; \\ N = 14 &: \quad -x_2^3x_3 + x_2^2x_3^2 + x_1^2x_2x_3 + x_1x_2x_3^2 - x_1x_3^3 = 0 \qquad (4,2) \\ N = 15 &: \quad x_1^2x_2^2 + x_1^2x_2x_3 + x_1^2x_3^2 - x_1x_2^3 - x_1x_2^2x_3 - x_1x_2x_3^2 + x_2^3x_3 = 0 \ . \end{aligned}$$

Remarque. Pour $N = 11 , 15$ , ces équations figurent dans [1] . Par contre, pour $N = 14$ , l'équation donnée dans [1] est fausse ; nous l'avons rectifiée ici.

Le cas $\boxed{N = 11}$ a été déjà traité par Billing-Mahler. Ces auteurs commencent par obtenir -à partir de l'équation (4,2)- le modèle $Y_1(11)$ dans la forme normale de Weierstrass. On a ainsi :

$$Y_1(11) : \quad y^2 = x^3 - 16.27x + 19.16.27 \ .$$

Ils prouvent alors que le $\mathbb{Q}$-rang de $Y_1(11)$ est nul et que le groupe de points exceptionnels est un groupe cyclique d'ordre 5 dont tous les éléments sont des points paraboliques ; ce qui implique que $\varepsilon_1(11) = 0$ . Nous nous bornerons donc ici aux cas $N = 14 , 15$ . Commençons par calculer le modèle désingularisé $Y_1(N)$ .

II. - $\boxed{N = 14}$ . De (4,2) , on déduit l'équation affine

$$-y^3 + y^2 + x^2y + xy - x = 0 \ ,$$

cubique qui admet le point rationnel $(0,0)$ ; la tangente en ce point coupe la cubique en $(0,1)$ . Si on amène l'origine en ce point, on a la nouvelle équation.

$$- y^3 + x^2y - 2y^2 + x^2 + xy - y = 0 \quad . \qquad (4,3)$$

Si on coupe cette courbe par la droite $y = tx$ , les abscisses des points d'intersection (autres que $(0,0)$) sont données par l'équation :

$$(-t^3+t)x^2 + (-2t^2+t+1)x - t = 0 \quad ,$$

c'est-à-dire

$$x = \frac{2t^2 - t - 1 \pm \sqrt{-4t^3+t^2+2t+1}}{-2t^3 - 2t} \quad .$$

La valeur $x$ est rationnelle si et seulement si le discriminant est un carré. Donc les points rationnels de (4,3) sont en correspondance birationnelle avec ceux de la courbe

$$v^2 = - 4t^3 + t^2 + 2t + 1 \quad .$$

D'où, finalement, par une transformation linéaire (et sous forme affine) :

$$Y_1(14) : \quad y^2 = x(x^2-3^3.11x + 2^5.3^4) \qquad (4,4)$$

III. - $\boxed{N = 15}$ . Faisons dans (4,2) la transformation monoïdale

$$x_1 = x'_2x'_3 \quad , \qquad x_2 = x'_1x'_3 \quad , \qquad x_3 = x'_1x'_2 \quad .$$

En simplifiant (et en changeant de notations) nous obtenons l'équation affine

$$y + y^2 + y^3 - x - xy - xy^2 + x^2 = 0 \quad .$$

Appliquant la transformation birationnelle $\xi = y/(x-1)$ , $\eta = 1/(x-1)$ , nous obtenons la nouvelle équation

$$\eta^2 + \xi^3 - \xi^2 - \eta\xi + \eta = 0 \quad .$$

D'où, par une transformation linéaire (et sous forme affine) :

$$Y_1(15) \quad : \quad y^2 = x(x^2-3^3.7x+2^4.3^4) \quad . \qquad (4,5)$$

## §2 - ETUDE DE $Y_1(N)_{\mathbb{Q}}$ .

I. - $\mathbb{Q}$-rang de $Y_1(N)$ . On a déjà signalé dans le chapitre III, §2, remarque 1, que pour $N = 11$ , $14$ , $15$ les courbes $Y_o(N)$ et $Y_1(N)$ sont isogènes. Donc, de la proposition 3.1, on déduit que pour ces trois valeurs, le $\mathbb{Q}$-rang de $Y_1(N)$ est 0 . On peut aussi procéder directement comme pour les courbes $Y_o(N)$ du chapitre III. Voir aussi notre note [24] pour la valeur $N = 15$ .

II. - Calcul des points exceptionnels.

Pour les trois valeurs de $N$ étudiées, $Y_1(N)_{\mathbb{Q}}$ se réduit donc à sa partie de torsion. Les points exceptionnels peuvent être calculés comme dans le §3 du chapitre III. Ainsi, les courbes $Y_1(14)$ , $Y_1(15)$ données par les équations (4,4) et (4,5) admettent les solutions exceptionnelles :

$$N = 14 \quad : \quad (\infty) \quad (0,0) \quad (2^2.3^2, \pm 2^2.3^3) \quad (2^3.3^2, \pm 2^3.3^3)$$

$$N = 15 \quad : \quad (\infty) \quad (0,0) \quad (2^2.3^2, \pm 2^2.3^3)$$

qui constituent un groupe cyclique d'ordre 6 et 4 respectivement. Donc

$$\rho_1(14) = 6 \qquad \rho_1(15) = 4 \quad .$$

III. - Calcul de $\sigma_1(N)$ .

La méthode de Billing et Mahler permet immédiatement de déterminer si une solution de (4,2) correspond à un point parabolique ou non (voir [1]).

Ainsi les courbes $B_{14}$ et $B_{15}$ données par (4,2) possèdent, au moins, les points rationnels paraboliques

$$N = 14 : (0,0,1) \quad (0,1,1) \quad (1/2,1/2,1) \quad (1,0,0) \quad (1,1,0) \quad (1,-1,0)$$

$$N = 15 : (0,1,0) \quad (0,0,1) \quad (1,0,0) \quad (1,1,0)$$

Comme $Y_1(14)$ (resp. $Y_1(15)$) possède seulement 6 (resp. 4) points rationnels, on doit avoir

$$\sigma_1(14) = 6 \quad , \quad \sigma_1(15) = 4 \quad .$$

§3 - CONCLUSION.

I. - Des résultats antérieurs, on déduit par différence (voir (4,1)) :

$$\varepsilon_1(14) = \varepsilon_1(15) = 0 \ ,$$

et donc

Proposition 4.1.

Pour $N = 14$ , $15$ , $\mathcal{E}_1(N)_{\mathbb{Q}}$ est vide .

Compte tenu de la définition de $\mathcal{E}_1(N)$ (chapitre II, §3,II) et des résultats de Billing-Mahler cités ci-dessus (pour $N = 11$), on a

Théorème A.

Il n'existe aucune courbe elliptique définie sur $\mathbb{Q}$ admettant un un point rationnel sur $\mathbb{Q}$ d'ordre $N = 11$ , $14$ , $15$ .

II. - Remarques : la proposition 4.1 montre la validité de la conjecture d'Ogg lorsque $p_1(N) = 1$ . Pour les valeurs de $N$ telles que $p_1(N) > 1$ , il n'existe pas de méthode d'étude générale. Pour certaines valeurs de $N$ , on peut "remplacer" $Y_1(N)$ par $Y_o(N)$ : c'est ce que nous avons fait par anticipation au chapitre III pour $N = 19$ , $27$ , $32$ , $36$ , $49$ , et cette méthode permet également de conclure pour $N = 26$ (voir [31]) ; en effet, on peut prouver que tous les points de $Y_o(26)$ rationnels sur $\mathbb{Q}$ sont paraboliques : donc $\varepsilon_o(26) = 0$ et a fortiori $\varepsilon_1(26) = 0$ : il n'existe pas de courbe elliptique sur $\mathbb{Q}$ ayant un point rationnel sur $\mathbb{Q}$ d'ordre 26 . Cette méthode s'applique aussi à $N = 37$ (voir [26]) : $Y_o(37)$ a pour équation affine $y^2 = -x^6 - 9x^4 - 4x^2 + 37$ , et possède quatre points rationnels sur $\mathbb{Q}$ ,

dont deux sont paraboliques ; ainsi, $\epsilon_o(37) = 2$ : il existe deux classes de courbes elliptiques sur $\mathbb{Q}$ ayant un sous-groupe cyclique rationnel sur $\mathbb{Q}$ d'ordre 37 ; on peut prouver que ces sous-groupes ne sont pas engendrés par un point rationnel ; donc : il n'existe pas de courbe elliptique sur $\mathbb{Q}$ admettant un point rationnel sur $\mathbb{Q}$ d'ordre 37 .

Dans le même ordre d'idées, citons encore deux résultats récents :

i) $\boxed{N = 17}$ . Dans ce cas $p_1(17) = 5$ , $p_o(17) = 1$ . Ogg [16] obtient, à partir de la courbe $B_{17}$ de Billing et Mahler, la courbe elliptique auxiliaire d'équation

$$y^2 = -4x^3 + 9x^2 - 4x ,$$

courbe isogène à $Y_o(17)$ et donc de $\mathbb{Q}$-rang 0 . En étudiant cette courbe, Ogg obtient le résultat suivant : Il n'existe pas de courbe elliptique définie sur $\mathbb{Q}$ et admettant un point rationnel sur $\mathbb{Q}$ d'ordre 17 .

ii) $\boxed{N = 13,16,18}$ . Pour ces valeurs, $p_1(N) = 2$ et $p_o(N) = 0$ ; Ogg [17] par des calculs relatifs à $J_1(N)_{\mathbb{Q}}$ , partie rationnelle de la jacobienne de $Y_1(N)$ , démontre le résultat suivant : Il n'existe pas de courbe elliptique définie sur $\mathbb{Q}$ et admettant un point rationnel sur $\mathbb{Q}$ d'ordre $N = 13$ , 16 , 18 . (Bien entendu, la non-existence de points d'ordre $N = 13$ implique la non-existence de points d'ordre 26) .

# BIBLIOGRAPHIE


[1] - G. BILLING & K. MAHLER : "On exceptional points on cubic curves". (J. London Math. Soc., 15 (1940).

[2] - A. BOREL, B. CHOWLER,... : "Seminar on complex multiplication" (Lecture Notes in Mathematics, 21, Springer, 1966).

[3] - J.W.S. CASSELS : "Diophantine equations with special reference to elliptic curves". (J. London Math. Soc., 41, 1966).

[4] - V.A. DEM'JANENKO : "Sur la torsion des courbes elliptiques" (en russe) (Izvestiia Akad. Nauk SSSR, 35, 1971).

[5] - R. FRICKE : "Elliptische Funktionen" (Leipzig, 1922).

[6] - A. GELFOND & I. LINNIK : "Méthodes élémentaires dans la théorie analytique des nombres" (Gauthier-Villars, 1965).

[7] - J.R. JOLY & J. TENA AYUSO : "Sous-groupes rationnels et points rationnels d'ordre fini sur certaines courbes elliptiques". (Comptes rendus Acad. Sci., Paris, 275 pp. 241-243, 1972)

[8] - J.R. JOLY & J. TENA AYUSO : "Rationalité des point paraboliques de $\Gamma_o(N)$ . Application aux courbes elliptiques sur $\mathbb{Q}$ ". (Comptes rendus Acad. Sci., Paris, 275, pp. 487-490, 1972).

[9] - G. LIGOZAT : "Fonction L des courbes modulaires" (Séminaire Delange-Pisot-Poitou, 1969-70, n°9).

[10] - C.E. LIND : Thèse (Uppsala, 1940).

[11] - E. LUTZ : "Sur l'équation $y^2 = x^3 - Ax - B$ dans les corps $p$-adiques". (Journal de Crelle, 177, 1937)


.../...

[12] - L.J. MORDELL : "Diophantine Equations"
(Academic Press, 1969).

[13] - T. NAGELL : "Solution de quelques problèmes dans la théorie arithmétique des cubiques planes du premier genre"
(Vid. Akad. Skrifter, Oslo, 1935).

[14] - T. NAGELL : "Recherches sur l'arithmétique des cubiques planes du premier genre dans un domaine de rationalité quelconque".
(Nova Acta Regiae Uppsala, 1952).

[15] - A.P. OGG : "Modular Forms and Dirichlet Series"
(Benjamin, 1969).

[16] - A.P. OGG : "Rational points of finite order on elliptic curves"
(Inventiones Math., 12, 1971).

[17] - A.P. OGG : "Rational points on certain elliptic modular curves"
(A.M.S. Symposium on Analytic Number Theory, St Louis, 1972).

[18] - P. ROQUETTE : "Analytic theory of elliptic functions over local fields".
(Vandenhoeck & Ruprecht, 1970).

[19] - E.S. SELMER : "The rational solutions of the diophantine equation $y^2 = \xi^3 - D$ for $|D| \leq 100$"
(Math. Scand., 4, 1956).

[20] - G. SHIMURA : "Arithmetic theory of automorphic functions"
(Princeton University Press, 1971).

[21] - P. SWINNERTON-DYER : "The conjectures of Birch and Swinnerton-Dyer, and of Tate"
(Proceeding of a conference on local fields, Springer, 1967).

[22] - J. TENA AYUSO : "Sur une démonstration élémentaire du théorème de Hasse"
(Séminaire de Théorie des Nombres, Grenoble, 1971).

[23] - J. TENA AYUSO : "Sur l'existence d'un point rationnel d'ordre N sur une courbe elliptique"
(Séminaire de Théorie des Nombres, Grenoble, 1972).

.../...

[24] - J. TENA AYUSO : "Points rationnels d'ordre 15 sur une courbe elliptique".
(Comptes rendus Acad. Sci. Paris, 274, pp. 1760-1763, 1972).

[25] - J. VELU : "Courbes elliptiques sur $\mathbb{Q}$ ayant bonne réduction en dehors de $\{11\}$"
(Comptes rendus Acad. Sci. Paris, 273, pp. 73-75, 1971)

[26] - J. VELU : "Les points rationnels de $X_0(37)$"
(Journées Arithmétiques, Grenoble, 1973).

[27] - H. WEBER : "Lehrbuch der Algebra"
(Leipzig, 1908).

[28] - Y. HELLEGOUARCH : "Courbes elliptiques et équation de Fermat".
(Thèse, Besançon, 1972).

[29] - B. MAZUR : "Arithmétique des courbes elliptiques sur les corps cyclotomiques".
(Orsay, 1970).

[30] - B. MAZUR : "Rational points of abelian varieties with values in towers of number fields"
(Inventiones math., 18, 1972).

[31] - B. MAZUR & J. VELU : "Courbes de Weil de conducteur 26"
(Comptes rendus Acad. Sci. Paris, 275, pp. 743-747, 1972).

-o-o-o-

# LISTE DES PROFESSEURS

Président : Monsieur Michel SOUTIF
Vice-Président : Monsieur Gabriel CAU

## PROFESSEURS TITULAIRES

| | | |
|---|---|---|
| MM. | ANGLES D'AURIAC Paul | Mécanique des fluides |
| | ARNAUD Georges | Clinique des maladies infectieuses |
| | ARNAUD Paul | Chimie |
| | AUBERT Guy | Physique |
| | AYANT Yves | Physique approfondie |
| Mme | BARBIER Marie-Jeanne | Electrochimie |
| MM. | BARBIER Jean-Claude | Physique expérimentale |
| | BARBIER Reynold | Géologie appliquée |
| | BARJON Robert | Physique nucléaire |
| | BARNOUD Fernand | Biosynthèse de la cellulose |
| | BARRA Jean-René | Statistiques |
| | BARRIE Joseph | Clinique chirurgicale |
| | BENOIT Jean | Radioélectricité |
| | BERNARD Alain | Mathématiques Pures |
| | BESSON Jean | Electrochimie |
| | BEZES Henri | Chirurgie générale |
| | BLAMBERT Maurice | Mathématiques Pures |
| | BOLLIET Louis | Informatique (IUT B) |
| | BONNET Georges | Electrotechnique |
| | BONNET Jean-Louis | Clinique ophtalmologique |
| | BONNET-EYMARD Joseph | Pathologie médicale |
| | BONNIER Etienne | Electrochimie Electrométallurgie |
| | BOUCHERLE André | Chimie et Toxicologie |
| | BOUCHEZ Robert | Physique nucléaire |
| | BOUSSARD Jean-Claude | Mathématiques Appliquées |
| | BRAVARD Yves | Géographie |
| | BRISSONNEAU Pierre | Physique du Solide |
| | BUYLE-BODIN Maurice | Electronique |
| | CABANAC Jean | Pathologie chirurgicale |
| | CABANEL Guy | Clinique rhumatologique et hydrologie |
| | CALAS François | Anatomie |
| | CARRAZ Gilbert | Biologie animale et pharmacodynamie |
| | CAU Gabriel | Médecine légale et Toxicologie |
| | CAUQUIS Georges | Chimie organique |
| | CHABAUTY Claude | Mathématiques Pures |
| | CHARACHON Robert | Oto-Rhino-Laryngologie |
| | CHATEAU Robert | Thérapeutique |
| | CHENE Marcel | Chimie papetière |
| | COEUR André | Pharmacie chimique |
| | CONTAMIN Robert | Clinique gynécologique |
| | COUDERC Pierre | Anatomie Pathologique |
| | CRAYA Antoine | Mécanique |
| Mme | DEBELMAS Anne-Marie | Matière médicale |
| MM. | DEBELMAS Jacques | Géologie générale |
| | DEGRANGE Charles | Zoologie |
| | DESRE Pierre | Métallurgie |
| | DESSAUX Georges | Physiologie animale |
| | DODU Jacques | Mécanique appliquée |
| | DOLIQUE Jean-Michel | Physique des plasmas |
| | DREYFUS Bernard | Thermodynamique |
| | DUCROS Pierre | Cristallographie |
| | DUCOIS Pierre | Clinique de Dermatologie et Syphiligraphie |
| | FAU René | Clinique neuro-psychiatrique |
| | FELICI Noël | Electrostatique |
| | GAGNAIRE Didier | Chimie physique |
| | GALLISSOT François | Mathématiques Pures |
| | GALVANI Octave | Mathématiques Pures |
| | GASTINEL Noël | Analyse numérique |
| | GEINDRE Michel | Electroradiologie |
| | GERBER Robert | Mathématiques Pures |
| | GIRAUD Pierre | Géologie |
| | KLEIN Joseph | Mathématiques Pures |
| Mme | KOFLER Lucie | Botanique et Physiologie végétale |
| MM. | KOSZUL Jean-Louis | Mathématiques Pures |
| | KRAVTCHENKO Julien | Mécanique |
| | KUNTZMANN Jean | Mathématiques Appliquées |
| | LACAZE Albert | Thermodynamique |
| | LACHARME Jean | Biologie végétale |
| | LAJZEROWICZ Joseph | Physique |
| | LATREILLE René | Chirurgie générale |
| | LATURAZE Jean | Biochimie pharmaceutique |
| | LAURENT Pierre | Mathématiques Appliquées |
| | LEDRU Jean | Clinique médicale B |
| | LLIBOUTRY Louis | Géophysique |
| | LOUP Jean | Géographie |
| Mle | LUTZ Elisabeth | Mathématiques Pures |
| | MALGRANGE Bernard | Mathématiques Pures |
| | MALINAS Yves | Clinique obstétricale |
| | MARTIN-NOEL Pierre | Séméiologie médicale |
| | MASSEPORT Jean | Géographie |
| | MAZARE Yves | Clinique médicale A |
| | MICHEL Robert | Minéralogie et Pétrographie |
| | MOURIQUAND Claude | Histologie |
| | MOUSSA André | Chimie nucléaire |
| | NEEL Louis | Physique du Solide |
| | OLLENDA Paul | Botanique |
| | PAUTHENET René | Electrotechnique |
| | PAYAN Jean-Jacques | Mathématiques Pures |
| | PEBAY-PEYROULA Jean-Claude | Physique |
| | PERRET René | Servomécanismes |
| | PILLET Emile | Physique industrielle |
| | RASSAT André | Chimie systématique |
| | RENARD Michel | Thermodynamique |
| | REULOS René | Physique industrielle |
| | RINALDI Renaud | Physique |
| | ROGET Jean | Clinique de pédiatrie et de puériculture |
| | SANTON Lucien | Mécanique |
| | SEIGNEURIN Raymond | Microbiologie et Hygiène |
| | SENGEL Philippe | Zoologie |
| | SILBERT Robert | Mécanique des fluides |
| | SOUTIF Michel | Physique générale |
| | TANCHE Maurice | Physiologie |
| | TRAYNARD Philippe | Chimie générale |
| | VAILLAND François | Zoologie |
| | VALENTIN Jacques | Physique Nucléaire |
| | VAUQUOIS Bernard | Calcul électronique |
| Mme | VERAIN Alice | Pharmacie galénique |
| M. | VERAIN André | Physique |
| Mme | VEYRET Germaine | Géographie |
| MM. | VEYRET Paul | Géographie |
| | VIGNAIS Pierre | Biochimie médicale |
| | YOCCOZ Jean | Physique nucléaire théorique |

## PROFESSEURS ASSOCIES

| | | |
|---|---|---|
| MM. | BULLEMER Bernhard | Physique |

## PROFESSEURS SANS CHAIRE

| | | |
|---|---|---|
| MM. | BEAUDOING André | Pédiatrie |
| Mme | BERTRANDIAS Françoise | Mathématiques Pures |
| MM. | BERTRANDIAS Jean-Paul | Mathématiques appliquées |
| | BIAREZ Jean-Pierre | Mécanique |
| | BONNETAIN Lucien | Chimie minérale |
| Mme | BONNIER Jane | Chimie générale |
| MM. | DEPASSEL Roger | Mécanique des Fluides |
| | DEPORTES Charles | Chimie minérale |
| | GAUTHIER Yves | Sciences biologiques |
| | GAVEND Michel | Pharmacologie |
| | GERMAIN Jean Pierre | Mécanique |
| | GIDON Paul | Géologie et Minéralogie |
| | GLENAT René | Chimie organique |
| | HACQUES Gérard | Calcul numérique |
| | JANIN Bernard | Géographie |
| Mme | KAHANE Josette | Physique |
| MM. | MULLER Jean-Michel | Thérapeutique |
| | PERRIAUX Jean-Jacques | Géologie et minéralogie |
| | POULOUJADOFF Michel | Electrotechnique |
| | REBECQ Jacques | Biologie (CUS) |
| | REVOL Michel | Urologie |
| | REYMOND Jean-Charles | Chirurgie générale |
| | ROBERT André | Chimie papetière |
| | DE ROUGEMONT Jacques | Neurochirurgie |
| | SARRAZIN Roger | Anatomie et chirurgie |
| | SARROT-REYNAULD Jean | Géologie |
| | SIBILLE Robert | Construction Mécanique |
| | SIROT Louis | Chirurgie générale |
| Mme | SOUTIF Jeanne | Physique générale |

## MAITRES DE CONFERENCES ET MAITRES DE CONFERENCES AGREGES

| | | |
|---|---|---|
| Mle | AGNIUS-DELORD Claudine | Physique pharmaceutique |
| | ALARY Josette | Chimie analytique |
| MM. | AMBLARD Pierre | Dermatologie |
| | AMBROISE-THOMAS Pierre | Parasitologie |
| | ARMAND Yves | Chimie |
| | BEGUIN Claude | Chimie organique |
| | BELORIZKY Elie | Physique |
| | BENZAKEN Claude | Mathématiques Appliquées |
| | BILLET Jean | Géographie |
| | BLIMAN Samuel | Electronique (EIE) |
| | BLOCH Daniel | Electrotechnique |
| Mme | BOUCHE Liane | Mathématiques (CUS) |
| MM. | BOUCHET Yves | Anatomie |
| | BOUVARD Maurice | Mécanique des Fluides |
| | BRODEAU François | Mathématiques (IUT B) |
| | BRUGEL Lucien | Energétique |
| | BUISSON Roger | Physique |
| | BUTEL Jean | Orthopédie |
| | CHAMOAZ Edmond | Biochimie médicale |
| | CHAMPETIER Jean | Anatomie et organogénèse |
| | CHIAVERINA Jean | Biologie appliquée (EFP) |
| | CHIBON Pierre | Biologie animale |
| | COHEN-ADDAD Jean-Pierre | Spectrométrie physique |
| | COLOMB Maurice | Biochimie médicale |
| | CONTE René | Physique |
| | COULOMB Max | Radiologie |
| | CROUZET Guy | Radiologie |
| | DURAND Francis | Métallurgie |
| | DUSSAUD René | Mathématiques (CUS) |
| Mme | ETERRADOSSI Jacqueline | Physiologie |
| MM. | FAURE Jacques | Médecine légale |
| | GENSAC Pierre | Botanique |
| | GIDON Maurice | Géologie |
| | GRIFFITHS Michaël | Mathématiques Appliquées |
| | GROULADE Joseph | Biochimie médicale |
| | HOLLARD Daniel | Hématologie |
| | HUGONOT Robert | Hygiène et Médecine préventive |
| | IDELMAN Simon | Physiologie animale |
| | IVANES Marcel | Electricité |
| | JALBERT Pierre | Histologie |
| | JOLY Jean-René | Mathématiques Pures |
| | JOUBERT Jean-Claude | Physique du Solide |
| | JULLIEN Pierre | Mathématiques Pures |
| | KAHANE André | Physique générale |
| | KUHN Gérard | Physique |
| | LACOUME Jean-Louis | Physique |
| Mme | LAJZEROWICZ Jeannine | Physique |
| MM. | LANCIA Roland | Physique atomique |
| | LE JUNTER Noël | Electronique |
| | LEROY Philippe | Mathématiques |
| | LOISEAUX Jean-Marie | Physique Nucléaire |
| | LONGEQUEUE Jean-Pierre | Physique Nucléaire |
| | LUU DUC Cuong | Chimie Organique |
| | MACHE Régis | Physiologie végétale |
| | MAGNIN Robert | Hygiène et Médecine préventive |
| | MARECHAL Jean | Mécanique |
| | MARTIN-BOUYER Michel | Chimie (CUS) |
| | MAYNARD Roger | Physique du Solide |
| | MICHOULIER Jean | Physique (I.U.T. "A") |
| | MICOUD Max | Maladies infectieuses |
| | MOREAU René | Hydraulique (INP) |
| | NEGRE Robert | Mécanique |
| | PARAMELLE Bernard | Pneumologie |
| | PECCOUD François | Analyse (IUT B) |
| | PEFFEN René | Métallurgie |
| | PELMONT Jean | Physiologie animale |
| | PERRET Jean | Neurologie |
| | PERRIN Louis | Pathologie expérimentale |
| | PFISTER Jean-Claude | Physique du Solide |
| | PHELIP Xavier | Rhumatologie |
| Mle | PIERY Yvette | Biologie animale |
| MM. | RACHAIL Michel | Médecine interne |
| | RACINET Claude | Gynécologie et obstétrique |
| | RENAUD Maurice | Chimie |
| | RICHARD Lucien | Botanique |
| Mme | RINAUDO Marguerite | Chimie macromoléculaire |
| MM. | ROMIER Guy | Mathématiques (IUT B) |
| | SHOM Jean Claude | Chimie Générale |
| | STIEGLITZ Paul | Anesthésiologie |
| | STOEBNER Pierre | Anatomie pathologique |
| | VAN CUTSEM Bernard | Mathématiques Appliquées |
| | VEILLON Gérard | Mathématiques Appliquées (INP) |
| | VIALON Pierre | Géologie |
| | VOOG Robert | Médecine interne |
| | VROUSSOS Constantin | Radiologie |
| | ZADWORNY François | Electronique |

## MAITRES DE CONFERENCES ASSOCIES

| | | |
|---|---|---|
| MM. | BOUDOURIS Georges | Radioélectricité |
| | CHEEKE John | Thermodynamique |
| | YACOUB Mahmoud | Médecine légale |

## CHARGES DE FONCTIONS DE MAITRES DE CONFERENCES

VU,

Grenoble, le

Le Président de la thèse,

C. CHABAUTY

VU, et permis d'imprimer

Grenoble, le

Le Président de l'Université scientifique et médicale,

M. SOUTIF